课件下载：www.tup.com.cn

- 数据加密技术
- 网络操作系统安全
- 数据库安全
- PKI技术、防火墙技术
- 网络扫描和网络监听
- Internet安全、VPN和IPSec

计算机网络安全技术与应用



主　编　雷渭侣

副主编　王兰波

清华大学出版社

计算机网络安全技术与应用

主编　雷渭侣

副主编　王兰波

编著　师　平　许丽娟　李　康

清华大学出版社

北　京

内 容 简 介

本书将计算机网络安全技术的基本理论与实际应用相结合，系统地介绍了计算机网络安全的基本概念以及网络安全体系结构、数据加密技术、网络操作系统安全、数据库与数据的安全、PKI 技术、防火墙工作原理及应用、计算机病毒防治、入侵检测系统、Internet 安全、VPN 和 IPSec 技术以及无线网络安全技术，各章均配有小结、练习与思考题，便于教学和自学。此外，附录部分还给出了网络安全实验的建议及题目。

本书内容安排合理，逻辑性强，语言表达通俗易懂，实例典型实用，可作为高等院校信息学科应用型本科学生计算机网络安全技术课程的教材，也可供从事计算机网络安全维护及管理的工程技术人员阅读参考。

图书在版编目（CIP）数据

计算机网络安全技术与应用/雷渭侣主编．—北京：清华大学出版社，2010.1

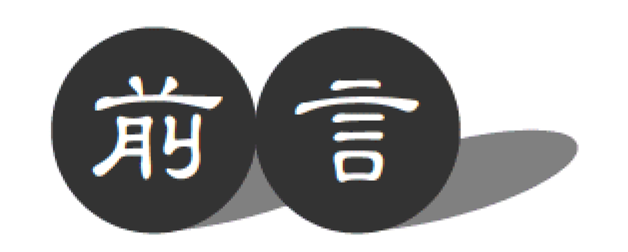
ISBN 978-7-302-21366-6

I. 计… II. 雷… III. 计算机网络–安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 190337 号

责任编辑：陈仕云 王 飞 纪文远
封面设计：张 岩
版式设计：杨 洋
责任校对：姜 彦
责任印制：
出版发行：清华大学出版社 **地 址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编：**100084
社 总 机：010-62770175 **邮 购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经 销：全国新华书店
开 本：185×260 **印 张：**23.25 **字 数：**537 千字
版 次：2010 年 1 月第 1 版 **印 次：**2010 年 1 月第 1 次印刷
印 数：1～4000
定 价：32.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。
联系电话：010-62770177 转 3103 产品编号：030852-01



随着 Internet 和 Intranet 技术的广泛应用，计算机网络资源共享进一步加强，但与此同时网络安全问题（既有来自外部的黑客攻击，也有来自内部的威胁）也变得日益突出，网络安全面临重大挑战。事实上，资源共享和信息安全历来就是一对矛盾，而计算机网络的开放性决定了网络安全问题是先天存在的，TCP/IP 框架基本上是不设防的。那么如何切实有效地保护计算机网络安全呢？您将从本书中找到答案。

本书根据作者多年从事本课程教学的讲稿，以及近几年来主编出版的 3 本计算机网络教材，并结合计算机网络安全技术的实际应用，综合计算机网络安全技术的发展现状编写而成。本书可作为普通高等院校计算机专业本科生计算机网络安全技术课程的教材，也可供信息学科非计算机专业本科生、成人教育学生、职业技术学院学生参考、学习。参考学时为 32～48 学时，其中含上机 6 学时。

本书最突出的特点是把计算机网络安全技术的基本理论、基本知识与实际应用技术和基本技能融为一体；紧密结合当前技术的新发展，在阐述理论知识的同时侧重实用性；力求在讲述概念和原理时做到严格、准确、精练。为便于教学，每章均附有小结、练习与思考题，画龙点睛地归纳该章精髓。

本书共包括 10 章和 1 个附录。第 1 章主要描述计算机网络安全的定义、目标、特征和安全策略，计算机网络安全的漏洞与威胁，网络安全体系结构，网络安全措施，网络安全评价标准等；第 2 章着重介绍数据加密技术，其中包括传统密码技术、对称和公开密钥密码体制、数字签名、密钥管理算法等；第 3 章重点介绍操作系统安全，其中包括 Windows NT 操作系统安全、UNIX/Linux 操作系统安全等；第 4 章介绍数据库与数据的安全，其中包括数据库安全的基本概念、数据库的安全特性、数据库的安全保护、Web 数据库的安全、SQL Server 数据库的安全；第 5 章介绍 PKI 技术，其中包括口令认证方法、身份识别与鉴别、PKI 的概念、证书权威 CA、PKI 应用举例；第 6 章介绍防火墙工作原理及应用，其中包括防火墙概述、防火墙技术、防火墙体系结构、防火墙的选型与产品简介、瑞星个人防火墙；第 7 章主要介绍计算机病毒防治，其中包括计算机病毒的特点与分类、恶意代码、计算机病毒的检测与清除、计算机病毒的现状和发展趋势；第 8 章主要介绍入侵检测系统，其中包括入侵检测原理与结构、网络扫描和网络监听、几种商用入侵检测系统；第 9 章重点介绍 Internet 安全、VPN 和 IPSec，其中包括 TCP/IP 协议及其安全、Web 站点安全、Web 电子商务安全、黑客与网络攻击、电子邮件系统的安全、虚拟专用网、IPSec 安全模式；第 10 章主要介绍无线网络的安全，其中包括无线网络标准、无线局域网有线等价保密安全机

制、无线局域网有线等价保密安全漏洞、无线局域网安全威胁、无线保护接入机制。在附录部分，分别给出了对网络安全实验的建议及题目、名词术语的英文缩写对照表、一些极具参考价值的网址。

本书撰写分工如下：第 1 章、第 2 章和第 10 章由雷渭侣教授执笔，并负责全书的统稿和主编工作；第 6 章和第 7 章由王兰波副教授执笔，并负责副主编工作；第 3 章由李康老师执笔；第 4 章和第 8 章由许丽娟讲师执笔；第 5 章和第 9 章由师平讲师执笔，并负责全书电子教案的制作。

在本书的立项、大纲编写和内容的确定以及全书的编写过程中得到了清华大学出版社各位老师的大力支持和帮助，在此表示衷心的感谢。同时，对曾参与制定本书大纲及为本书提供过宝贵意见和建议的老师和同学同样表示衷心的感谢。

由于作者水平有限，书中难免存在错误之处，恳请广大读者批评指正。

雷渭侣

2009 年 8 月于广州

目录

第 1 章

绪　　论

本章学习要求：

（1）掌握网络安全定义及其特征。
（2）掌握网络安全漏洞。
（3）掌握网络安全威胁。
（4）掌握网络安全的体系结构。
（5）了解网络安全措施。
（6）了解其他国家信息安全评价标准。
（7）了解我国信息安全评价标准。

重点和难点：

（1）重点：掌握网络安全的定义、特征、漏洞和威胁。
（2）难点：掌握网络安全的体系结构概念。

随着 Internet 的迅速发展、广泛应用，网络的触角深入到政治、经济、文化、军事、意识形态和社会生活等各个方面，其影响与日俱增、无处不在，由此也宣告了网络社会化时代的到来。在我们尽情享受网络带来的快捷、便利服务的同时，全球范围内针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量也在持续不断增加，对国家安全、经济和社会生活造成了极大的威胁。因此，网络安全已成为当今世界各国共同关注的焦点。

事实上，资源共享和网络安全本身就是相互矛盾的，随着资源共享的加强，网络安全问题必然日益突出。因此，如何使计算机网络系统不受破坏，提高系统的安全性已成为人们关注且必须认真对待的问题。每个计算机用户都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全、稳定地运行。

网络安全问题涉及到数据加密技术、网络操作系统、数据库与数据访问技术、PKI 技术、防火墙工作原理及应用、计算机病毒防治、入侵检测系统、Internet 安全等内容，我们将在以后各章中一一介绍。

1.1 计算机网络安全基本概念

1.1.1 什么是网络安全

所谓“安全”，字典中的定义是为防范间谍活动或蓄意破坏、犯罪、攻击而采取的措施。将安全的一般含义限定在计算机网络范畴，网络安全就是为防范计算机网络硬件、软件、数据偶然或蓄意被破坏、篡改、窃听、假冒、泄露、非法访问并保护网络系统持续有效工作的措施总和。

1. 网络安全保护范围

网络安全与信息安全、计算机系统安全和密码安全密切相关，但涉及的保护范围不同。信息安全所涉及的保护范围包括所有信息资源；计算机系统安全将保护范围限定在计算机系统硬件、软件、文件和数据范畴，安全措施通过限制使用计算机的物理场所和利用专用软件或操作系统来实现；密码安全是信息安全、网络安全和计算机系统安全的基础与核心，也是身份认证、访问控制、拒绝否认和防止信息窃取的有效手段。网络安全与信息安全、计算机系统安全和密码安全的关系如图 1-1 所示。

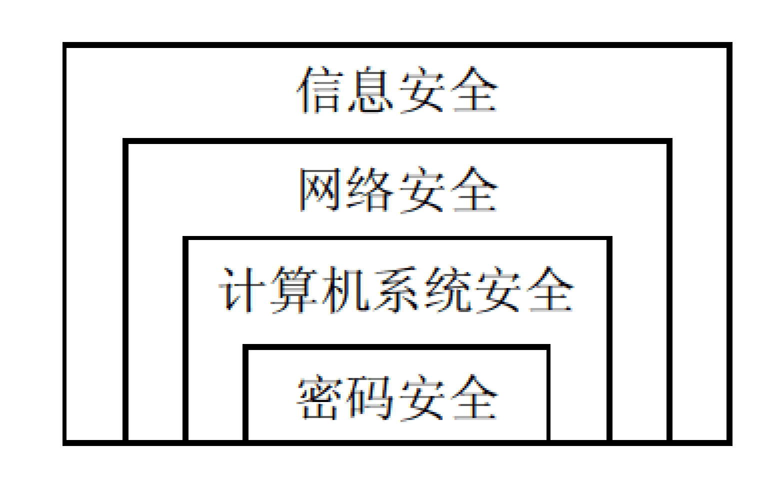


图 1-1 网络安全保护范围

2. 网络安全侧重点

事实上，网络安全也可以看成是计算机网络上的信息安全，凡涉及网络信息的可靠性、保密性、完整性、有效性、可控性和拒绝否认性的理论、技术与管理都属于网络安全的研究范畴，只是不同人员或部门对网络安全关注的侧重点有所不同。网络安全研究人员更关注从理论上采用数学方法精确描述安全属性，通过安全模型来解决网络安全问题。网络安全工程人员则从实际应用角度出发，对成熟的网络安全解决方案和新型网络安全产品更感兴趣，注重于各种安全防范工具、操作系统防护技术和安全应急处理措施。网络安全评估人员较多关注的是网络安全评价标准、安全等级划分、安全产品测评方法与工具、网络信息采集以及网络攻击技术。网络管理或网络安全管理人员通常更关心网络安全管理策略、身份认证、访问控制、入侵检测、网络安全审计、网络安全应急响应和计算机病毒防治等安全技术，因为他们的主要职责便是配置与维护网络，即在保护授权用户方便快捷地访问网络资源的同时，必须防范非法访问、病毒感染、黑客攻击、服务中断和垃圾邮件等各种威胁，一旦系统遭到破坏，造成数据或文件丢失，能够采取相应的网络安全应急响应措施予以补救。对国家安全保密部门来说，必须了解网络信息泄露、窃听和过滤的各种技术手段，避免涉及国家政治、军事、经济等重要机密信息的无意或有意泄露；抑制和过滤威胁国家安全的反动与邪教等意识形态信息传播，以免给国家的稳定带来不利的影响，甚至危

害到国家安全。对公共安全部门而言，应当熟悉国家和行业部门颁布的常用网络安全监察法律法规、网络安全取证、网络安全审计、知识产权保护、社会文化安全等技术，一旦发现窃取或破坏商业机密信息、软件盗版、电子出版物侵权、色情与暴力信息传播等各种网络违法犯罪行为，能够取得可信的、完整的、准确的、符合国家法律法规的诉讼证据。军事人员则更关心信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击和网络病毒传播等网络安全综合技术，以此夺取网络信息优势、扰乱敌方指挥系统、摧毁敌方网络基础设施，打赢未来信息战争。当然，并非只有这些专业部门、人员需要关注网络安全问题，我们每个人都无法置身度外。在网络为工作、生活和学习带来便捷的同时，我们更加关心如何保护个人隐私和商业信息不被窃取、篡改、破坏和非法存取，确保网络信息的保密性、完整性、有效性和拒绝否认性。

1.1.2 网络安全目标

网络安全的最终目标就是通过各种技术与管理手段实现网络信息系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性。可靠性（Reliability）是所有信息系统正常运行的基本前提，通常指信息系统能够在规定的条件与时间内完成规定功能的特性。可控性（Controllability）是指信息系统对信息内容和传输具有控制能力的特性。拒绝否认性（No-repudiation）也称为不可抵赖性或不可否认性，是指通信双方不能抵赖或否认已完成的操作和承诺（如利用数字签名防止通信双方否认曾经发送和接收信息的事实）。在多数情况下，网络安全更侧重强调网络信息的保密性、完整性和有效性。

1. 保密性

保密性（Confidentiality）是指信息系统防止信息非法泄露的特性，信息只限于授权用户使用。保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现。信息加密是防止信息非法泄露的最基本手段。口令加密可以防止密码被盗，保护密码是防止信息泄露的关键。如果密码以明文形式传输，在网络上窃取密码非常简便，轻而易举就可以办到。事实上，大多数网络安全防护系统都采用了基于密码的技术，密码一旦泄露，就意味着整个安全防护系统的全面崩溃。机密文件和重要电子邮件在 Internet 上传输也需要加密，加密后的文件和邮件即使被劫持，尽管多数加密算法是公开的，但由于没有正确密钥进行解密，劫持的密文仍然是不可读的。此外，机密文件即使不在网络上传输，也应该进行加密，否则窃取密码就可以获得机密文件。对机密文件加密，可以提供双重保护。

2. 完整性

完整性（Integrity）是指信息未经授权不能改变的特性。完整性与保密性强调的侧重点不同，保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，信息在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息。影响信息完整性的因素主要有硬件故障、软件故障、网络故障、灾害事件、入侵

攻击和计算机病毒等。保障信息完整性的技术主要有安全通信协议、密码校验和数字签名等。实际上，数据备份是防范信息完整性受到破坏的最有效恢复手段。

3. 有效性

有效性（Availability）是指信息资源容许授权用户按需访问的特性（信息系统面向用户服务的安全特性）。信息系统只有持续有效，授权用户才能随时、随地根据自己的需要访问信息系统提供的服务。有效性在强调面向用户服务的同时，还必须进行身份认证与访问控制，只有合法用户才能访问限定权限的信息资源。一般而言，如果网络信息系统能够满足保密性、完整性和有效性 3 个安全目标，在通常意义下就可认为信息系统是安全的。

1.1.3 网络安全的特征

网络安全主要涉及系统的可靠性，软件及数据的完整性、可用性和保密性等几方面。

（1）网络系统的可靠性（Reliability）

网络系统的可靠性是指保证网络系统不因各种因素的影响而中断正常工作。

（2）软件及数据的完整性（Integrity）

软件及数据的完整性是指保护网络系统中存储和传输的软件（程序）及数据不被非法操作，即保证数据不被插入、替换和删除，数据分组不丢失、乱序以及数据库中的数据或系统中的程序不被破坏等。

（3）软件及数据的可用性（Availability）

软件及数据的可用性是指在保证软件和数据完整性的同时，还要使其可被正常利用和操作。

（4）软件及数据的保密性（Confidentiality）

软件及数据的保密主要是指利用密码技术对软件和数据进行加密处理，保证在系统中存储和在网络上传输的软件和数据不被无关人员识破。

1.1.4 网络安全策略

网络安全策略是保障机构网络安全的指导文件。一般而言，网络安全策略包括总体安全策略和具体安全管理实施细则。总体安全策略用于构建机构网络安全框架和战略指导方针，包括分析安全需求、分析安全威胁、定义安全目标、确定安全保护范围、分配部门责任、配备人力物力、确认违反策略的行为和相应的制裁措施。总体安全策略只是一个安全指导思想，还不能具体实施，在总体安全策略框架下针对特定应用制定的安全管理细则才规定了具体的实施方法和内容。

1. 安全策略总则

无论是制定总体安全策略，还是制定安全管理实施细则，都应当根据网络安全特点遵守均衡性、时效性和最小限度原则。

（1）均衡性原则

由于软件漏洞、协议漏洞、管理漏洞和网络威胁永远不可能消除，网络安全必定是计算机网络的永恒主题。无论制定多么完善的网络安全策略，还是使用多么先进的网络安全技术，网络安全也只是一个相对概念，因为世上没有绝对的安全系统。此外，网络易用性、网络效能与安全强度是一对天生的矛盾。夸大网络安全漏洞和威胁不仅会浪费大量投资，而且会降低网络易用性和网络效能，甚至有可能引入新的不稳定因素和安全隐患。忽视网络安全比夸大网络安全更加严重，有可能造成机构或国家重大经济损失，甚至威胁到国家安全。因此，网络安全策略需要在安全需求、易用性、效能和安全成本之间保持相对平衡，科学制定均衡的网络安全策略是提高投资回报和充分发挥网络效能的关键。

（2）时效性原则

由于影响网络安全的因素随时间有所变化，导致网络安全问题具有显著的时效性。例如，网络用户增加、信任关系发生变化、网络规模扩大、新安全漏洞和攻击方法不断暴露都是影响网络安全的重要因素。因此，网络安全策略必须考虑环境随时间的变化。

（3）最小限度原则

网络系统提供的服务越多，安全漏洞和威胁也就越多。因此，应当关闭网络安全策略中没有规定的网络服务；以最小限度原则配置满足安全策略定义的用户权限；及时删除无用账号和主机信任关系，将威胁网络安全的风险降至最低。

2. 安全策略内容

一般而言，大多数网络都是由网络硬件、网络连接、操作系统、网络服务和数据组成，网络管理员或安全管理员负责安全策略的实施，网络用户则应当严格按照安全策略的规定使用网络提供的服务。因此，在考虑网络整体安全问题时应主要从网络硬件、网络连接、操作系统、网络服务、数据、安全管理责任和网络用户几方面着手。

（1）网络硬件物理安全

核心网络设备和服务器应当设置防盗、防火、防水、防毁等物理安全设施以及温度、湿度、洁净、供电等环境安全设施。例如，每年因雷电击毁网络设施的事例层出不穷，这就要求位于雷电活动频繁地区的网络基础设施必须配备良好的防雷与接地装置。在规划物理安全设施时可参考《电子计算机机房设计规范》(GB 50174—1993)、《计算站场地安全要求》（GB 9361—1988)、《建筑物电子信息系统防雷技术规范》（GB 50343—2004)、《计算站场地技术条件》(GB 2887—1989)、《计算机机房用活动地板技术条件》(GB 6650—1986)等国家技术标准。

核心网络设备和服务器最好集中放置在中心机房，其优点是便于管理与维护，也容易保障设备的物理安全，更重要的是能够防止直接通过端口窃取重要资料。防止信息空间扩散也是规划物理安全的重要内容，除光纤之外的各种通信介质、显示器以及设备电缆接口都不同程度地存在电磁辐射现象，利用高性能电磁监测和协议分析仪有可能在几百米范围内将信息复原，对于涉及国家机密的信息必须考虑电磁泄露防护技术。例如，铺设电缆采用金属导管屏蔽，计算机和显示器最好使用符合美国瞬态电磁脉冲辐射标准 TEMPEST

（Transient Electromagnetic Pulse Emanation Standard，美国国家安全部制定的计算机信息泄漏安全防护标准）的产品，尽可能减小因电磁辐射导致失密的危险。我国也先后颁布了国家公共安全保密标准《计算机信息系统设备电磁泄漏发射限值》（GGBBl—1999）、《计算机信息系统设备电磁泄漏发射测试方法》（GGBB2—1999）和国家保密标准《涉密信息设备使用现场的电磁泄漏发射防护要求》（BMB5—2000）。

（2）网络连接安全

网络连接安全主要考虑网络边界的安全，例如，内部网（Intranet）与外部网（Extranet）、Internet 有连接需求，可使用防火墙和入侵检测技术双层安全机制来保障网络边界的安全。内部网安全主要通过操作系统安全和数据安全策略来保障；由于网络地址转换（Network Address Translator，NAT）技术能够对 Internet 屏蔽内部网地址，必要时也可以考虑使用 NAT 保护内部网私有 IP 地址。

对网络安全有特殊要求的内部网最好使用物理隔离技术保障网络边界的安全。根据安全需求，可以采用固定公用主机、双主机或一机两用等不同物理隔离方案。固定公用主机与内部网无连接，专用于访问 Internet，虽然使用不够方便，但能够确保内部主机信息的保密性。双主机指在一个机箱中配备两块主板、两块网卡和两个硬盘，在启动时由用户选择内部网或 Internet 连接，较好地解决了安全性与方便性的矛盾。一机两用隔离方案由用户选择接入内部网或 Internet，但不能同时接入两个网络，虽然成本低廉、使用方便，但仍然存在泄密的可能性。

（3）操作系统安全

操作系统安全应重点考虑计算机病毒、特洛伊木马（Trojan Horse）和入侵攻击威胁。计算机病毒是隐藏在计算机系统中的程序；具有自我繁殖、相互感染、激活再生、隐藏寄生、迅速传播等特点；以降低计算机系统性能、破坏系统内部信息或破坏计算机系统运行为目的。截至目前，已发现有两万多种不同类型的病毒。病毒传播途径已经从移动存储介质转向 Internet，在网络中以指数增长规律迅速扩散，诸如邮件病毒、Java 病毒和 ActiveX 病毒都给网络病毒防治带来了新的挑战。而“特洛伊木马”与计算机病毒不同，它是一种未经用户同意私自驻留在正常程序内部、以窃取用户资料为目的的间谍程序。

目前并没有特别有效的计算机病毒和“特洛伊木马”程序防治手段，主要还是通过提高病毒防范意识、严格安全管理、安装性能优异的防、杀病毒软件及“特洛伊木马”专杀软件来尽可能减少病毒与木马入侵的机会。操作系统漏洞为入侵攻击提供了条件，因此经常升级操作系统、防病毒软件和木马专杀软件是提高操作系统安全性的最有效、最简便方法。

（4）网络服务安全

目前，网络提供的电子邮件、文件传输、Usenet 新闻组、远程登录、域名查询（虽然用户并不直接使用域名查询服务，但域名查询通过将主机名转换成主机 IP 地址为其他网络服务奠定了基础）、网络打印和 WWW（World Wide Web）服务都存在大量的安全隐患。由于不同网络服务的安全隐患和安全措施不同，应当在分析网络服务风险的基础上，为每一种网络服务分别制定相应的安全策略细则。

（5）数据安全

根据数据机密性和重要性的不同，一般将数据分为关键数据、重要数据、有用数据和非重要数据，以便对不同类型数据采取不同的保护措施。关键数据是指直接影响网络系统正常运行或无法再次得到的数据，例如操作系统和关键应用程序等；重要数据是指具有很高机密性或高使用价值的数据，例如国防或国家安全部门涉及国家机密的数据、金融部门涉及用户的账目数据等；有用数据一般是指网络系统经常使用但可以从其他地方复制的数据；非重要数据则是很少使用而且很容易得到的数据。由于任何安全措施都不可能保证网络绝对安全或不发生故障，在网络安全策略中除考虑重要数据加密之外，还必须考虑关键数据和重要数据的备份。

目前数据备份使用的介质主要是磁带、硬盘和光盘。因磁带具有容量大、技术成熟、成本低廉等优点，大容量数据备份多选用磁带存储介质。随着硬盘价格不断下降，网络服务器转而采用硬盘作为存储介质。目前流行的硬盘数据备份技术主要有磁盘镜像和冗余磁盘阵列（Redundant Arrays of Inexpensive Disks，RAID）。磁盘镜像技术能够将数据同时写入型号与格式相同的主磁盘和辅助磁盘，而 RAID 是专用服务器广泛使用的磁盘容错技术。大型网络常采用光盘库、光盘阵列和光盘塔作为存储设备，但光盘特别容易划伤，导致数据读出错误，因此数据备份使用更多的还是磁带和硬盘存储介质。

（6）安全管理责任

由于人是制定和执行网络安全策略的主体，所以必须明确网络安全管理责任人。小型网络可由网络管理员兼任网络安全管理职责，但大型网络、电子政务、电子商务、电子银行或其他要害部门的网络应配备专职网络安全管理责任人。网络安全管理采用技术与行政相结合的手段，主要对授权、用户和资源进行管理，其中授权是网络安全管理的重点。安全管理责任包括行政职责、网络设备、网络监控、系统软件、应用软件、系统维护、数据备份、操作规程、安全审计、病毒防治、入侵跟踪、恢复措施、内部人员和网络用户等与网络安全相关的各种功能。

（7）网络用户安全责任

网络安全不只是网络安全管理员的事，网络用户对网络安全也负有不可推卸的责任。网络用户应特别注意不能私自将调制解调器（Modem）接入 Internet；不要下载未经安全认证的软件和插件；确保本机没有安装文件和打印机共享服务；不要使用脆弱性口令；经常更换口令等。

1.1.5　下一代网络安全

网络安全威胁多种多样，随着环境的变化和技术的发展，其形式和手段也在不断变化。经典网络安全技术以威胁为出发点而设计，对于威胁的多样性和不断变化的特性有着明显的局限性。从网络系统业务出发、以管理和监控为核心手段、以经典网络安全技术为重要补充的网络安全技术和方案成为近几年网络安全技术发展的主流。

1. 下一代网络安全体系

下一代网络安全技术既吸纳了传统网络安全技术中最精华的部分，也发展了大部分有价值的方法，同时创新了许多新的问题解决思路。从网络系统的业务和结构特点出发，以综合增强网络系统的安全性能为目的是下一代网络安全技术解决网络安全问题的基本思想。下一代网络安全技术体系如图 1-2 所示。

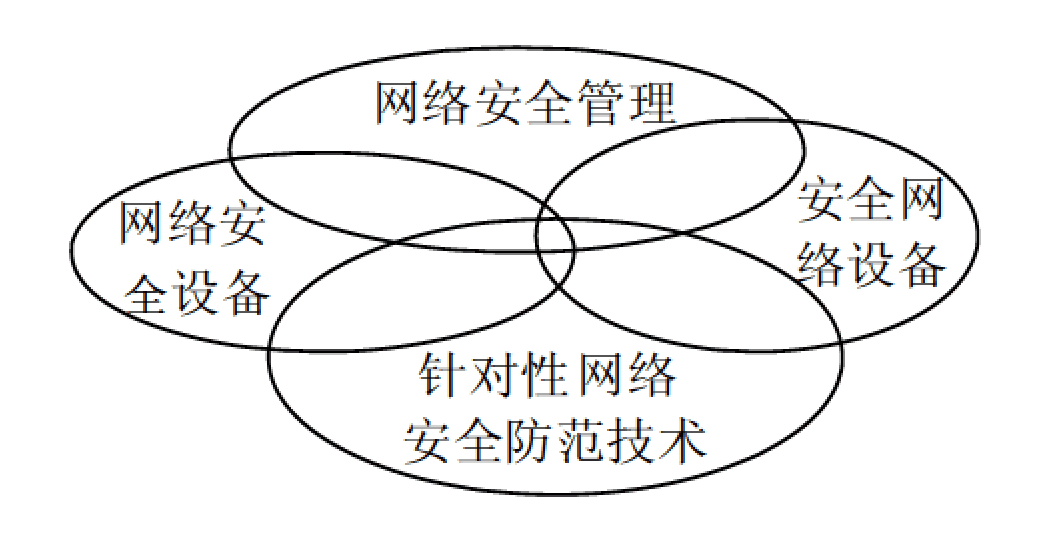


图 1-2 下一代网络安全技术体系

图 1-2 中 4 类不同解决网络安全的技术代表了下一代网络安全技术的 4 种相辅相成的不同思路。网络安全设备技术是从网络系统不同环节，以专用安全设备和安全系统的形式解决安全问题；安全网络设备技术则立足在原有网络设备的基础上，增强网络设备自身的安全能力，必要的时候增加相应的安全模块，从而提高网络系统整体的安全性，使网络建设从设计开始就尽可能成为安全的网络；针对性网络安全防范技术则是针对少数流行且较难防范的安全威胁的专用技术，例如分布式拒绝服务攻击 DDoS；网络安全管理技术将管理的理念直接应用于网络安全，通过对业务、网络设备、安全设备、威胁、异常现象、缺陷等与网络安全相关因素的管理，使得网络系统运行在安全、可控的状态中。

网络安全设备、安全网络设备和针对性网络安全防范技术是经典网络安全技术的直接延伸，也是下一代网络安全技术的基础，网络安全管理则是下一代网络安全技术的核心。

2. 经典网络安全延伸

（1）网络安全设备

网络安全设备泛指以专用设备或专用安全系统形式、提供专门网络安全服务的网络安全技术。这里既包括传统的防火墙技术、VPN 技术、IDS 和病毒防范系统等，也包括新发展的类似 DDoS 攻击防范设备，当然传统技术的综合和延伸也多是这种形式。

（2）网络安全增强

通过在基础网络设备、网络服务器系统或网络终端上增加提供安全功能的软件和硬件组件，提高网络系统的安全特性、抵御可能的网络攻击的方法，我们称之为网络安全增强。安全增强之后的网络系统通常也称为安全网络系统。安全交换机、安全路由器、安全服务器和安全终端则是网络安全增强的具体表现形式。

（3）针对性防范技术

少数网络攻击手段威胁大、易于实施却难以防范，导致其经常发生；而且攻击所破坏的不是网络系统中简单的某个方面的安全缺陷，对攻击的防范手段不能简单地整合到某类提供专门安全功能的技术中，例如通过防火墙、VPN 来解决。

有针对性地设计专用系统，不同程度地解决问题，是处理这类威胁的有效方法，例如用以防范 DoS 攻击的流量迁移和过滤技术等。

3. 网络安全管理

网络管理技术是网络维护的核心技术之一，安全网管技术则是在更高一个层面上（安

全）实现网络管理和维护的技术，近几年在传统网络管理技术的基础上，对安全信息的处理、安全响应模式和统一协调等方面发展较快。安全网管技术需要应用多种不同的网络安全技术和设备，对网络系统进行安全、合理、有效和高效的维护和管理。一般意义下，安全网管技术需要实施一个基于多层次安全防护的策略，将网络访问控制、入侵检测、病毒检测和网络流量管理等安全技术应用到内部网中，在统一的管理和控制下，各种安全技术彼此补充、相互配合，对网络行为进行检测和控制，形成一个安全策略集中管理、安全检查机制分散布置的分布式安全防护体系结构，从而达到对内部网进行安全保护和管理的目的。

安全网络管理技术牵涉到网络安全技术和管理的方方面面，从法律、法规到规章制度，从网络审计、网络监控到风险评估，乃至更广义的防火墙和 IDS 系统等安全设备本身也是安全网络管理的一种手段。以下仅对扫描、监控和审计等技术作进一步说明。

系统和网络的扫描和评估因其可预知主体受攻击的可能性、将要发生的行为和产生的后果，而受到网络安全业界的重视。这一技术的应用可帮助识别检测对象的系统资源，分析这一资源被攻击的可能指数，了解支撑系统本身的脆弱性，评估所有存在的安全风险。一些非常重要的专业应用网络（例如银行）哪怕遭受一次入侵，其损失也是无法承受的，因此对扫描和评估技术有着强烈的需求。

监控和审计是与网络管理直接挂钩的技术，主要是通过对网络通信过程中可疑、有害信息或行为进行记录以便为事后处理提供依据，从而对计算机网络犯罪人员形成一个强有力的威慑和最终达到提高网络整体安全性的目的。局域网监控系统是网络监控系统中的一大类，能够提供一套较好的内部网行为监控的机制，有效阻止来自内部网的安全威胁。不同企事业单位和不同性质的网络所提供的服务和业务之间差别很大，可能遭受的网络安全威胁不尽相同，这就需要网络监控技术针对不同的业务特性进行具体的监控。网络监控技术的专业性很强，不同的局域网监控系统，其功能表现可能完全不同。

1.2 网络安全漏洞与威胁

1.2.1 软件漏洞

软件漏洞（Flaw）是指在设计与编制软件时没有考虑对非正常输入进行处理或错误代码而造成的安全隐患，也称为软件脆弱性（Vulnerability）或软件隐错（Bug）。之所以产生软件漏洞，其主要原因在于软件设计人员不可能将所有输入都考虑周全，因此任何软件都不可避免地存在软件漏洞。软件产品通常在正式发布之前，都要相继发布 α 版本、β 版本和 γ 版本供反复测试使用，目的就是为了尽可能减少软件漏洞。

缓冲区溢出、特殊字符组合和操作系统多任务竞争是最常见的软件漏洞。除非正常输入和错误代码造成的软件漏洞之外，通常将软件配置不当造成的安全隐患也归类到软件漏洞范畴。例如，操作系统默认配置、脆弱性口令和系统后门等都是攻击首选的安全漏洞。

不同软件、同一软件的不同版本或不同运行环境，其软件漏洞各不相同，因此脱离具体软件和运行环境讨论软件漏洞毫无意义。此外，软件漏洞具有时效性，随着软件的广泛使用，软件漏洞将不断暴露出来。软件商通常会发布软件补丁修补已发现的软件漏洞，或在新版本中予以纠正。新版本软件在纠正旧版本软件的同时，有可能引入新的软件漏洞。随着软件使用时间的推移，已暴露的软件漏洞会不断消亡，新的软件漏洞将不断出现。

1.2.2 网络协议漏洞

网络协议漏洞类似于软件漏洞，是指网络通信协议不完善而导致的安全隐患。截至目前，Internet 上广泛使用的 TCP/IP 协议族中几乎所有协议都存在安全隐患，包括数据链路层的地址解析协议（Address Resolution Protocol，ARP）、逆向地址解析协议（Reverse Address Resolution Protocol，RARP）；网络层的网际协议（Internet Protocol，IP）、Internet 控制报文协议（Internet Control Messages Protocol，ICMP）、Internet 组管理协议（Internet Group Management Protocol，IGMP）；传输层的传输控制协议（Transfer Control Protocol，TCP）、用户数据报协议（User Datagram Protocol，UDP）、可靠数据协议（Reliable Data Protocol，RDP）；应用层的域名系统（Domain Name Systems，DNS）、文件传输协议（File Transfer Protocol，FTP）、超文本传输协议（Hypertext Transfer Protocol，HTTP）、简单邮件传输协议（Simple Message Transfer Protocol，SMTP）、远程登录协议 Telnet 等。

应用程序在 IEEE802.3 以太网（Ethernet）标准上采用 TCP/IP 协议传送数据时，用户数据通过传输层、网络层、数据链路层都要分别添加 TCP、IP 和载波监听多路访问/冲突检测（Carrier Sense Multiple Access/Collision Detect，CSMA/CD）头部信息。由于 IP 数据包封装在 CSMA/CD 帧内，位于数据链路层的网络接口驱动程序并不清楚有 IP 地址，而且也不理解 IP 地址格式，而主机在数据链路层采用 48 位介质访问控制 MAC 硬件地址实现数据通信，因此在数据通信之前必须首先获得目标主机的 MAC 地址，将源和目标主机的 MAC 地址封装在 CSMA/CD 帧头内，最终才能通过物理层介质达到传送数据的目的。ARP 协议的主要任务就是通过查询本机 ARP 缓冲表来获取目标 IP 地址对应的 MAC 地址。主机传送数据前，首先查询 ARP 缓冲表，如检索到目标 IP 地址，即将对应的 MAC 地址封装在帧头内；否则，在网段内发送一个 ARP 询问广播包，具有目标 IP 地址的主机将回送一个包含 MAC 地址的 ARP 应答包，源主机提取目标 MAC 地址并将其保存到 ARP 缓冲表。正是 ARP 协议的应答与地址映射机制导致了安全隐患，ARP 应答包完全可以假冒路由器、文件服务器或数据库服务器 IP 地址，再将目标设定为某台主机的 MAC 地址，接收 ARP 虚假应答包的主机就会将路由器、文件服务器或数据库服务器 IP 地址错误地映射成指定主机的 MAC 地址，结果是发往路由器、文件服务器或数据库服务器的数据包全部被传送到某台指定的主机。这种利用 ARP 协议应答与地址映射机制漏洞实施的攻击称为缓冲中毒攻击（Cache Poisoning）。

针对 TCP 协议三次握手初始连接和应答每个接收数据包安全漏洞，TCP 协议漏洞典型攻击有 Land 攻击、会话劫持（Hijack）攻击、TCP 序列号猜测攻击、同步洪流攻击（SYN

Flood)、TCP 状态转移和定时器拒绝服务攻击等。其中，UDP Fraggle 拒绝服务攻击是针对 UDP 协议漏洞的典型攻击之一，首先它将目标 IP 地址设置成目标网络的广播地址，然后通过伪造目标网络中某主机 UDP 广播数据包，使得广播域内所有主机向目标主机发送错误消息，目标主机将被错误消息所淹没，导致目标主机发生拒绝服务。Smurf 攻击利用 ICMP 回复漏洞和 IP 地址欺骗能够使广播域内数据流量巨增，从而导致目标主机拒绝为正常请求服务。ICMP 协议与 IP 协议都位于网络层，但 ICMP 报文是封装在 IP 数据报中传输的。Smurf 攻击类似于 UDP Fraggle 拒绝服务攻击，伪造源 IP 地址并将目标 IP 地址设置成目标网络的广播地址，通过向广播域发送类型为 8、代码为 0 的回应请求（echo）ICMP 报文，广播域内的所有主机都会向伪造的 IP 地址发送回应消息，大量回应消息不仅充斥广播域，而且将淹没目标主机。

截至 2004 年 9 月 1 日，专门从事安全漏洞名称标准化的公共漏洞披露机构（Common Vulnerability and Exposures，CVE）已发布 7616 个不同的安全漏洞，而新的安全漏洞仍在不断被披露。

1.2.3　安全管理漏洞

软件漏洞和网络协议漏洞是天生具有的，但由于安全管理疏漏产生的安全漏洞则完全是人为因素造成的。网络安全技术只是保证网络安全的基础，网络安全管理才是发挥网络安全技术的根本保证。因此，网络安全问题并不是一个纯技术问题，从网络安全管理角度看，网络安全首先应当是管理问题。事实上，国际标准化组织（International Organization for Standardization，ISO）也是将网络管理划分为故障、性能、配置、记账和安全管理 5 个领域，表明安全管理是网络管理的重要组成部分。

由于计算机网络包含各种网络设施、服务器、工作站和网络终端等设备，每个设备又可能安装了不同操作系统和应用软件，各自具有不同的安全隐患，导致网络安全隐患数量庞大且十分复杂，由此提升了网络安全管理的技术难度与成本，容易造成更多的安全管理疏漏。

其实只要提高安全管理意识，许多安全管理漏洞完全可以避免，例如常见的系统默认配置、脆弱性口令和信任关系转移等。系统默认配置主要考虑的是用户友好性，但方便使用的同时也就意味着更多的安全隐患。许多系统采用 123456 作为默认口令，用 Administrator 或 ChangMe 作为默认用户名，这些系统默认配置很容易被猜测。许多用户习惯以用户名或用户名的变形、自己或亲友生日、电话号码、身份证或员工号码、常用单词等作为口令，事实上这些口令都是典型的脆弱性口令。假设用出生 19××（0～99）年××（1～12）月××日（1～31）8 位数字作为口令，可能的组合数只有 100×12×31=37200 种，一般口令破解软件每秒至少可以搜索 4 万种组合。通常 8 位以上、字母大小写和数字混用的口令才是安全口令。

网络安全管理是在网络安全策略指导下为保护网络不受内外各种威胁而采取的一系列网络安全措施，网络安全策略则是根据网络安全目标和网络应用环境，为提供特定安全级

别保护而必须遵守的规则。因此，网络安全策略与网络应用环境密切相关，不同的应用环境需要制定不同的安全策略。如果将信任区的安全策略应用到非信任区，必然会产生众多的安全管理漏洞。如果将非信任区的安全策略应用到信任区，又会造成不必要的资金浪费。由此可见，网络安全是相对的，是建立在信任基础之上的，绝对的网络安全永远不存在。信任区与非信任区，或者安全区与非安全区的边界是基于信任关系划定的。在安全区内应当相信系统管理人员和内部用户不会滥用特权，并且具有良好的职业道德；但是当信任关系发生变化时，安全管理必须进行及时调整，否则会大大降低整个网络的安全性。

1.2.4 网络系统面临的威胁

网络系统面临的威胁主要来自外部的人为影响和自然环境的影响，其中包括对网络设备的威胁和对网络中信息的威胁。这些威胁主要表现为：非法授权访问、假冒合法用户、病毒破坏、线路窃听、黑客入侵、干扰系统正常运行、修改或删除数据等。这些威胁大致可分为无意威胁和故意威胁两大类。

1. 无意威胁

无意威胁是在无预谋的情况下破坏系统的安全性、可靠性或信息的完整性等。

无意威胁主要是由一些偶然因素引起的，例如软、硬件的机能失常，人为误操作，电源故障和自然灾害等。

人为的失误现象有：人为误操作，管理不善而造成系统信息丢失、设备被盗、火灾、水灾，安全设置不当而留下安全漏洞，用户口令不慎泄露，信息资源共享设置不当而被非法用户访问等。

自然灾害威胁是指由地震、风暴、泥石流、洪水、闪电雷击、虫鼠害及高温、各种污染等构成的威胁。

2. 故意威胁

故意威胁实际上就是“人为攻击”。由于网络本身存在脆弱性，因此总有某些人或某些组织想方设法利用网络系统达到某种目的。例如，从事工业、商业或军事情报搜集工作的“间谍”，他们对相应领域的网络信息是最感兴趣的，对网络系统的安全构成了主要威胁。

攻击者对系统的攻击范围从随便浏览信息到使用特殊技术对系统进行攻击，以便得到有针对性的信息。这些攻击又可分为被动攻击和主动攻击。

被动攻击是指攻击者只通过监听网络线路上的信息流获得信息内容，或获得信息的长度、传输频率等特征，以便进行信息流量分析攻击。被动攻击不干扰信息的正常流动，如被动地搭线窃听或非授权地阅读信息。被动攻击破坏了信息的保密性。

主动攻击是指攻击者对传输中的信息或存储的信息进行各种非法处理，有选择地更改、插入、延迟、删除或复制这些信息。主动攻击常用的方法有篡改程序及数据、假冒合法用户入侵系统、破坏软件和数据、中断系统正常运行、传播计算机病毒、耗尽系统的服务资源而造成拒绝服务等。主动攻击的破坏力更大，直接威胁到网络系统的可靠性以及信息的

保密性、完整性和可用性。

被动攻击不容易被检测到，因为它没有影响信息的正常传输，发送和接收双方均不容易觉察；但被动攻击比较容易防范，只要采用加密技术将传输的信息加密，即使该信息被窃取，非法接收者也不能识别信息的内容。

主动攻击较容易被检测到，但却难于防范。因为正常传输的信息如被篡改或伪造，接收方根据经验和规律可容易地觉察出来。除采用加密技术外，还要采用鉴别技术和其他保护机制和措施，才能有效地防止主动攻击。

被动攻击和主动攻击有以下 4 种具体类型，其中 3 种主动攻击类型如图 1-3 所示。

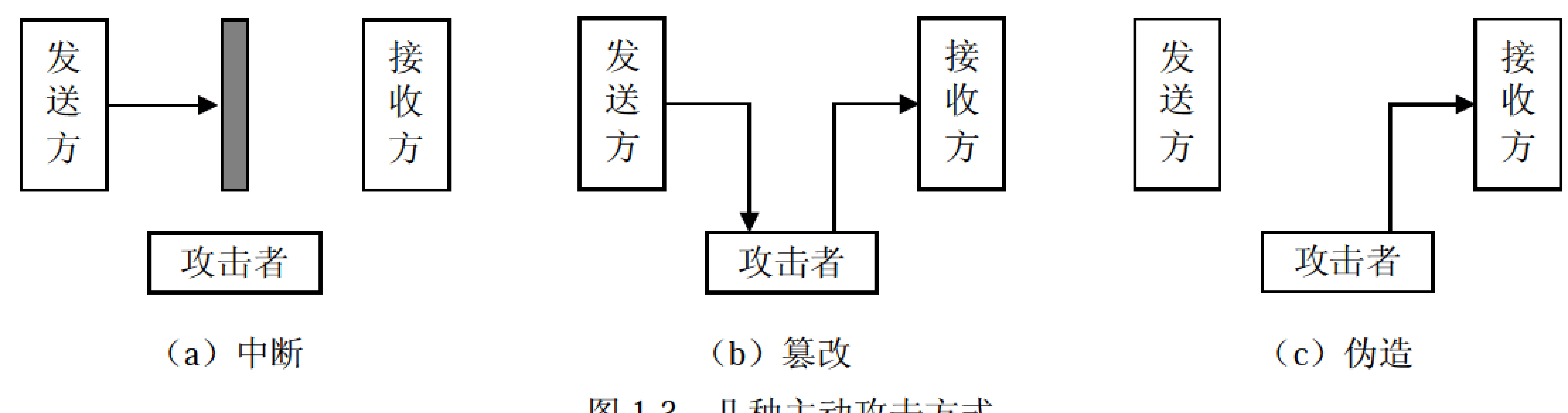


图 1-3　几种主动攻击方式

（1）窃听（interception）：攻击者未经授权而浏览了信息资源。这是对信息保密性的威胁。例如，通过搭线捕获线路上传输的数据等。

（2）中断（interruption）：攻击者中断正常的信息传输，使接收方收不到信息，正常的信息变得无用或无法利用。这是对信息可用性的威胁。例如，破坏存储介质、切断通信线路、入侵文件管理系统等。

（3）篡改（modification）：攻击者未经授权而访问了信息资源，并篡改了信息。这是对信息完整性的威胁。例如，修改文件中的数据、改变程序功能、修改传输的报文内容等。

（4）伪造（fabrication）：攻击者在系统中加入了伪造的内容。这也是对数据完整性的威胁。例如，向网络用户发送虚假信息、在文件中插入伪造的记录等。

1.3　网络安全体系结构

网络安全体系结构是网络安全层次的抽象描述。在大规模的网络工程建设、管理及基于网络安全系统的设计与开发过程中，需要从全局的体系结构角度考虑安全问题的整体解决方案，才能保证网络安全功能的完备性和一致性，降低安全代价和管理开销。这样一种网络安全体系结构对于网络安全解决方案的设计、实现与管理都有重要的意义。

网络安全是一个涉及范围较广的研究领域，人们一般都只是在该领域中的一个小范围内做自己的研究，开发能够解决某种特殊网络安全问题的方案。例如，有人专门研究加密和鉴别，有人专门研究入侵和检测，有人专门研究黑客攻击等。网络安全体系结构就是从系统化的角度去理解这些安全问题的解决方案，对研究、实现和管理网络安全的工作具有全局指导作用。

1.3.1 网络安全模型

网络安全的基本模型如图 1-4 所示。众所周知，通信双方在网络上传输信息，需要先在发、收方之间建立一条逻辑通道。这就要先确定从发送端到接收端的路由，再选择该路由上使用的执行通信的协议，例如 TCP/IP。

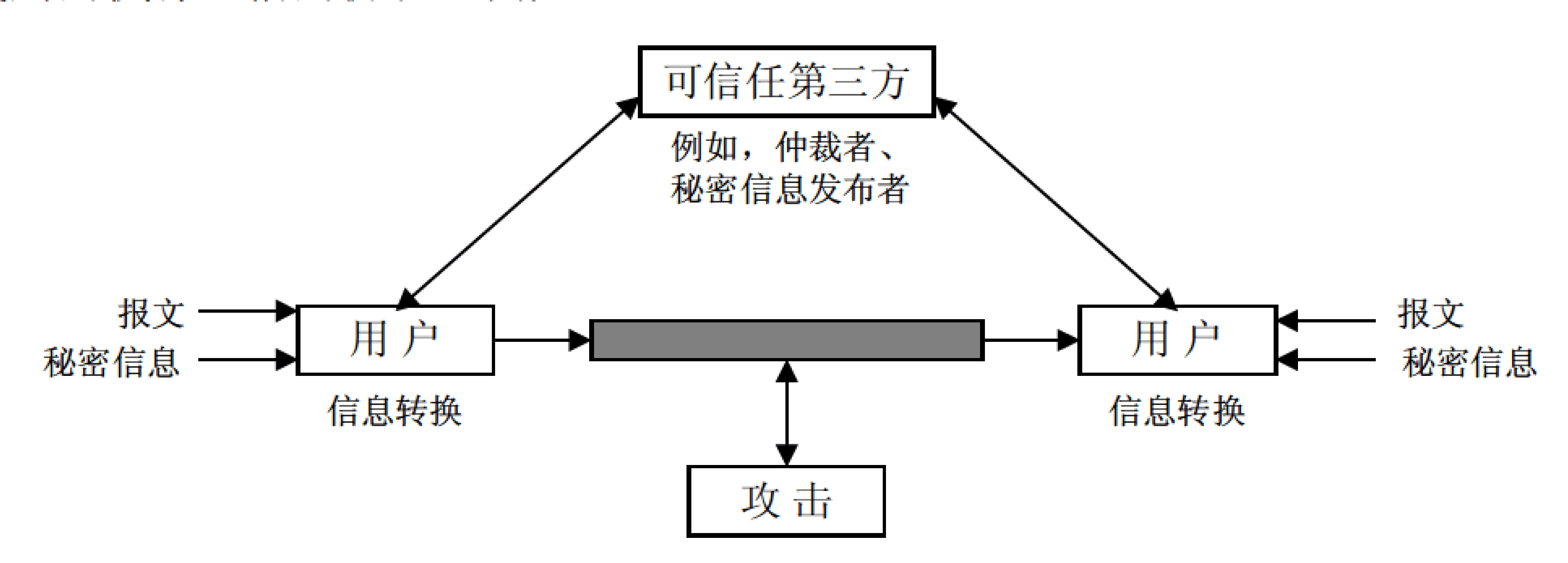


图 1-4 网络安全模型

为了在开放式的网络环境中安全地传输信息，需要对信息提供安全机制和安全服务。信息的安全传输包括两个基本部分：一是对发送的信息进行安全转换，例如信息加密，以便实现信息的保密性，或附加一些特征码，以便进行发送方身份验证等；二是发、收双方共享的某些秘密信息，例如加密密钥，除了对可信任的第三方外，对其他用户是保密的。

为了使信息安全地进行传输，通常需要一个可信任的第三方，其作用是负责向通信双方分发秘密信息，以及在双方发生争议时进行仲裁。

一个安全的网络通信方案必须考虑以下内容：

- 实现与安全相关的信息转换的规则或算法。
- 用于信息转换算法的秘密信息（例如，密钥）。
- 秘密信息的分发和共享。
- 使用信息转换算法和秘密信息获取安全服务所需的协议。

1.3.2 网络信息安全框架

网络信息安全可看成一个由多个安全单元组成的集合。其中，每个单元都是一个整体，包含了多个特性。一般来说，人们从 3 个主要特性——安全特性、安全层次和系统单元来理解安全单元。该安全单元集合可用一个三维安全空间来描述，如图 1-5 所示。该三维安全空间反映了信息系统安全需求和安全结构的共性。

1. 安全特性

安全特性指的是该安全单元可解决哪些安全威胁。信息安全特性包括保密性、完整性、可用性和认证安全性。

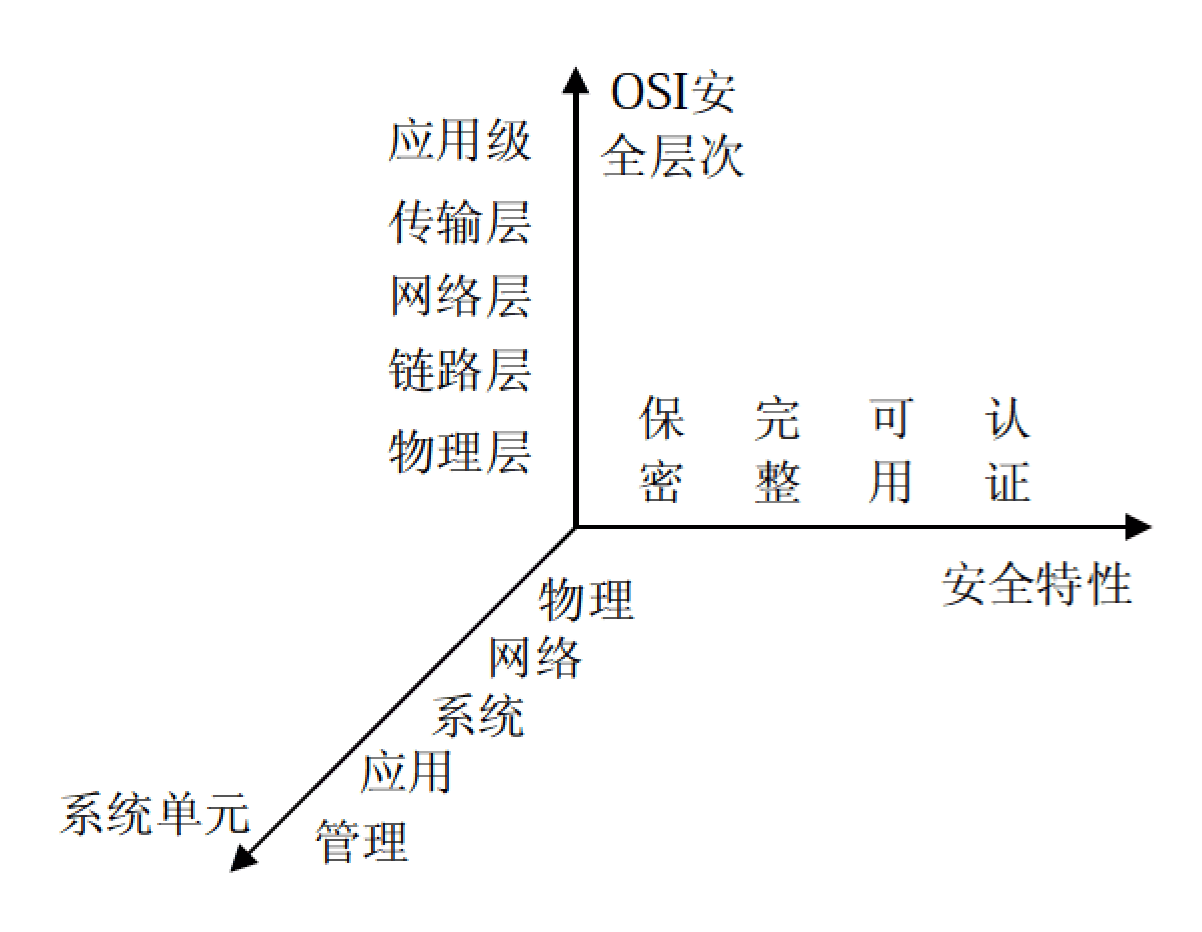


图 1-5　网络信息安全框架

（1）保密性主要是指保护信息在存储和传输过程中不被未授权的实体识别。例如，网上传输的信用卡账号和密码不被识破。

（2）完整性主要指信息在存储和传输过程中不被未授权的实体插入、删除、篡改和重发等，即信息的内容不会改变。例如，保证用户发给别人的电子邮件到接收端时内容没有改变。

（3）可用性是指不能由于系统受到攻击而使用户无法正常去访问他本来有权正常访问的资源。例如，保护邮件服务器安全，保证其不会因为遭到拒绝服务 DoS 攻击而无法正常工作，用户能正常收发电子邮件。

（4）认证安全性是指通过某些验证措施和技术，防止无权访问某些资源的实体通过某种特殊手段进入网络而进行访问。

2. 系统安全

系统安全是指该安全单元解决什么系统环境的安全问题。对于现代网络，系统单元涉及以下 5 个不同环境。

（1）物理单元

物理单元是指硬件设备、网络设备等，包含该特性的安全单元解决物理环境安全问题。

（2）网络单元

网络单元是指网络传输，包含该特性的安全单元解决网络协议造成的网络传输安全问题。

（3）系统单元

系统单元是指操作系统，包含该特性的安全单元解决端系统或中间系统的操作系统包含的安全问题（一般是指数据和资源在存储时的安全问题）。

（4）应用单元

应用单元是指应用程序，包含该特性的安全单元解决应用程序所包含的安全问题。

（5）管理单元

管理单元是指网络安全管理环境。网络管理系统对网络资源进行安全管理。

1.3.3 OSI 网络安全体系

1. OSI 概述

OSI 参考模型是国际标准化组织（ISO）为解决异种机互联而制定的开放式计算机网络层次结构模型，其最大优点是将服务、接口和协议这 3 个概念明确地区分开来。

ISO 提出 OSI 参考模型的目的，就是要使在各种终端设备之间、计算机之间、网络之间、操作系统进程之间以及人们之间互相交换信息的过程能够逐步实现标准化。参照这种参考模型进行网络标准化的结果，就是使得各个系统之间都是“开放”的，凡是遵守这一标准的系统之间都可以互联。ISO 还希望能够用这种参考模型来解决不同系统之间的信息交换问题，使不同系统之间也能交互工作，以实现分布式处理。

ISO 于 1989 年 2 月公布的 ISO7498-2《网络安全体系结构》文件给出了 OSI 参考模型的安全体系结构，简称 OSI 安全体系结构。这是一个普遍适用的安全体系结构，它对具体网络的安全体系结构具有指导意义，其核心内容是保证异构计算机系统之间远距离交换信息的安全。

OSI 安全体系结构主要包括网络安全机制和网络安全服务两方面的内容，下面分别介绍。

2. 网络安全机制

在 ISO7498-2《网络安全体系结构》文件中规定的网络安全机制有 8 项：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、信息量填充机制、路由控制机制和公证机制。

（1）加密机制

数据加密是提供信息保密的主要方法，可保护数据存储和传输的保密性。此外，加密技术和其他技术合作，可保证数据的完整性。

（2）数字签名机制

数字签名可解决传统手工签名中存在的安全缺陷，在电子商务中应用较广泛。数字签名主要解决否认问题（发送方否认他发送了信息）、伪造问题（某方伪造了文件却不承认）、冒充问题（冒充合法用户在网上发送文件）和篡改问题（接收方私自篡改文件内容）。

（3）访问控制机制

访问控制机制可以控制哪些用户可以访问哪些资源，对这些资源可以访问到什么程度。例如，非法用户企图访问资源，该机制就会加以拒绝，并将这一非法事件记录在审计报告中。访问控制可以直接支持数据的保密性、完整性、可用性，作用非常明显。

（4）数据完整性机制

数据完整性机制保护网络系统中存储和传输的软件（程序）和数据不被非法改变，例如被添加、删除、修改等。

（5）交换鉴别机制

交换鉴别机制主要是通过相互交换信息来确定彼此的身份。在计算机网络中，鉴别主要有站点鉴别、报文鉴别、用户和进程的认证等，通常采用口令、密码技术、实体的特征或所有权等手段进行鉴别。

（6）信息流填充机制

攻击者对传输信息的长度、频率等特征进行统计，然后进行信息流量分析，即可从中得到有用的信息。采用信息量填充机制，可保持系统信息量基本恒定，因此能防止攻击者对系统进行信息流量分析。

（7）路由控制机制

路由控制机制可以指定通过网络发送数据的路径，以便选择那些可信度高的节点传输信息。

（8）公证机制

公证机制就是在网络中设立一个公证机构，来中转各方交换的信息，并从中提取相关证据，以便对可能发生的纠纷作出仲裁。

3．网络安全服务

在《网络安全体系结构》文件中规定的网络安全服务有 5 项：鉴别服务、访问控制服务、数据完整性服务、数据保密性服务和非否认服务。

（1）鉴别服务

鉴别服务包括同等实体鉴别和数据源鉴别两种服务。

使用同等实体鉴别服务可以对两个同等实体（用户或进程）在建立连接和开始传输数据时进行身份的合法性和真实性验证，以防止非法用户的假冒或非法用户伪造连接初始化攻击。

数据源鉴别服务可对信息源点进行鉴别，以确保数据是由合法用户发出，以防假冒。

（2）访问控制服务

访问控制包括身份验证和权限验证。访问控制服务既可防止未授权用户非法访问网络资源，也可防止合法用户越权访问网络资源。

（3）数据完整性服务

数据完整性服务旨在防止非法用户对正常数据进行变更（例如，修改、插入、延时或删除），以及在数据交换过程中的数据丢失。数据完整性服务可分为以下 5 种情形，通过这些服务来满足不同用户、不同场合对数据完整性的要求。

① 带恢复功能的面向连接的数据完整性。

② 不带恢复功能的面向连接的数据完整性。

③ 选择字段面向连接的数据完整性。

④ 选择字段无连接的数据完整性。

⑤ 无连接的数据完整性。

（4）数据保密性服务

采用数据保密性服务的目的是保护网络中各通信实体之间交换的数据即使被非法攻击

者截获，也使其无法解读信息内容，以保证信息不失密。该服务也提供面向连接和无连接两种数据保密方式。保密性服务还提供给用户可选字段的数据保护和信息流安全，即对可能从观察信息流就能推导出的信息提供保护。信息流安全的目的是确保信息从源点到目的点的整个流通过程的安全。

（5）非否认服务

非否认服务可防止发送方发送数据后否认自己发送过数据，也可防止接收方接收数据后否认已接收过数据。它由两种服务组成：一是发送（源点）非否认服务，二是接收（交付）非否认服务。这实际上是一种数字签名服务。

1.3.4 P2DR 模型

P2DR 模型是一种常用的网络安全模型，如图 1-6 所示。P2DR 模型包含 4 个主要部分：安全策略、防护、检测和响应。防护、检测和响应组成了一个所谓的“完整”、“动态”的安全循环。在整体安全策略的控制和指导下，在综合运用防护工具（例如，防火墙、身份认证、加密等手段）的同时，利用检测工具（例如，漏洞评估、入侵检测等工具）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。P2DR 是由（Protection-Detection-Response，PDR）模型引申出的概念模型，增加了 Policy 功能，并突出了管理策略在信息安全工程中的主导地位。该模型指出：安全技术措施是围绕安全策略的具体需求有序地组织在一起，构架一个“动态”的安全防范体系。

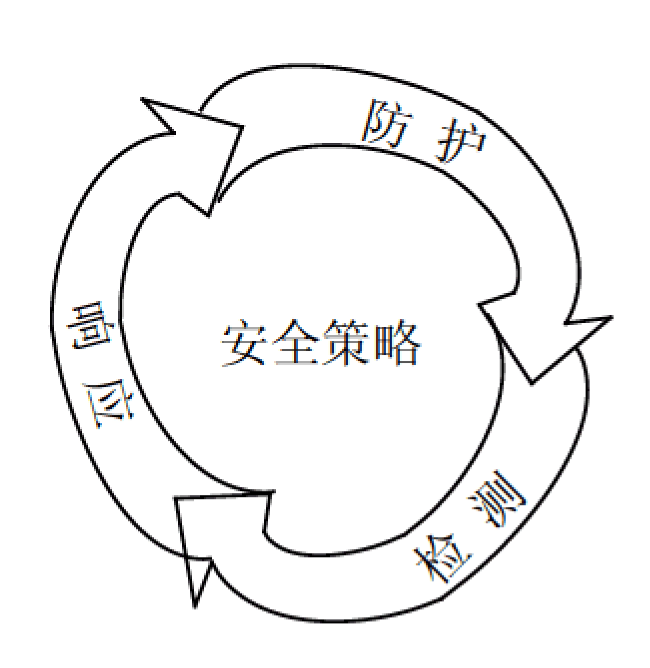


图 1-6 P2DR 网络安全模型

P2DR 模型中 4 个主要部分的内涵如下。

1. 安全策略

在考虑建立网络安全系统时，在了解了网络信息安全系统等级划分和评估网络安全风险后，接下来一个很重要的任务就是要制定一个网络安全策略。一个策略体系的建立包括安全策略的制定、安全策略的评估、安全策略的执行等。网络安全策略一般包括两部分：总体的安全策略和具体的安全规则。总体的安全策略用于阐述本部门网络安全的总体思想和指导方针；而具体的安全规则是根据总体安全策略提出的具体网络安全实施规则，用于说明网络上哪些活动是被允许的，哪些活动是被禁止的。由于安全策略是安全管理的核心，所以要想实施动态网络安全循环过程，必须制定网络系统的安全策略，所有的防护、检测、响应都是依据安全策略实施的，网络系统安全策略为安全管理提供了管理方向和支持手段。

2. 防护

防护就是根据系统可能出现的安全问题采取一些预防措施，通过一些传统的静态安全

技术及方法来实现。通常采用的主动防护技术有数据加密、身份验证、访问控制、授权和虚拟网络 VPN 技术，被动防护技术有防火墙技术、安全扫描、入侵检测、路由过滤、数据备份和归档、物理安全、安全管理等。

防护是 P2DR 模型中最重要的部分，通过它可以预防大多数的入侵事件。防护可分为 3 类：系统安全防护、网络安全防护和信息安全防护。系统安全防护是指操作系统的安全防护，即各个操作系统的安全配置、使用和打补丁等，不同操作系统有不同的防护措施和相应的安全工具；网络安全防护指网络管理的安全及网络传输的安全；信息安全防护指数据本身的保密性、完整性和可用性，数据加密就是信息安全防护的重要技术。

3. 检测

如果攻击者穿过防护系统，检测系统就会将其检测出来。例如，检测入侵者的身份，包括攻击源、系统损失等。防护系统可以阻止大多数的入侵事件，但不能阻止所有的入侵事件，特别是那些利用新的系统缺陷、新攻击手段的入侵。如果入侵事件发生，就要启动检测系统进行检测。

检测与防护有着根本的区别。防护主要是修补系统和网络缺陷，增加系统安全性能，从而消除攻击和入侵的条件，避免攻击的发生；而检测是根据入侵事件的特征进行的。因为黑客往往是利用网络和系统缺陷进行攻击的，因此入侵事件的特征一般与系统缺陷特征有关。在 P2DR 模型中，防护和检测具有互补关系。如果防护系统过硬，绝大部分入侵事件被阻止，那么检测系统的任务就会减少。

检测是动态响应的依据，也是强制落实安全策略的有力工具，通过不断地检测和监控网络系统，可发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。

4. 响应

系统一旦检测出入侵，响应系统就开始响应，进行事件处理。P2DR 中的响应就是在已知入侵事件发生后，进行的紧急响应（事件处理）。响应工作可由特殊部门——计算机紧急响应小组负责。世界上第一个计算机紧急响应小组简称 CERT（Computer Emergency Response Team），我国第一个计算机紧急响应小组是由中国教育与科研计算机网络建立的，简称 CCERT，而不同机构也有相应的计算机紧急响应小组。

响应的主要工作可分为两种：紧急响应和恢复处理。紧急响应就是当安全事件发生时采取相应的应对措施；恢复处理是指事件发生后，把系统恢复到原来的状态或比原来更安全的状态。

紧急响应在安全系统中占有重要的地位，是解决潜在安全问题最有效的办法。从某种意义上讲，安全问题就是要解决紧急响应和异常处理问题。要解决好紧急响应问题，就要制订好紧急响应方案，做好紧急响应方案中的一切准备工作。

恢复包括系统恢复和信息恢复两方面内容。系统恢复是指修补缺陷和消除后门，不让黑客再利用这些缺陷入侵系统。消除后门是系统恢复的一项重要工作。一般说来，黑客第一次入侵是利用系统缺陷，在入侵成功后，黑客会在系统中留下一些后门，例如安装木马

程序。因此，尽管缺陷可通过打补丁的方式修复，黑客还是可以通过留下的后门入侵系统。信息恢复是指恢复丢失的数据。丢失数据可能是由于黑客入侵所致，也可能是系统故障、自然灾害等原因所致。

P2DR 安全模型也存在一个明显的弱点，就是忽略了内在的变化因素。例如，人员的流动、人员的素质差异和策略贯彻的不稳定性。实际上，安全问题牵涉面广，除了涉及到防护、检测和响应，系统本身安全的“免疫力”的增强、系统和整个网络的优化，以及人员这个在系统中最重要角色的素质的提升，都是该安全模型没有考虑到的问题。

1.4 网络安全措施

实现网络安全，不但要靠法律的约束、安全的管理和教育，更重要的是要依靠先进的网络技术的支持。先进的网络安全技术是网络安全的根本保证。通常采用以下几类安全措施来保证计算机网络的安全：

1.4.1 安全立法

计算机犯罪是一种高技术犯罪活动，也是未来社会的主要犯罪形式之一，面对其日益严重的威胁，必须建立、健全相关的法律、法规进行约束，即通过建立、健全国际、国内和地方计算机信息安全法来减少计算机犯罪案件（例如，盗窃网络设施、非法入侵网络来破坏和盗窃信息资源、故意制造病毒破坏网络系统等）的发生。由于法律具有强制性、规范性、公正性、威慑性和权威性，因此它在很多方面具有不可代替的作用。制定并实施计算机信息安全法律，加强对计算机网络安全的宏观控制，对危害计算机网络安全的行为进行制裁，为网络信息系统提供一个良好的社会环境是十分必要的。

1．国外的计算机信息安全立法

在国际上，由于发达国家的计算机应用已非常普及，因此其计算机安全立法工作也早已进行。不同形式的法律，例如《计算机安全法》、《信息自由法》、《伪造访问设备和计算机欺骗与滥用法》、《数据保护法》、《计算机犯罪法》、《计算机软件保护法》、《电子资金转账法》、《保密法》、《个人隐私法》等均已出台，一些国家还将计算机犯罪与刑法、民法联系在一起，修改有关条款，颁布实施，收到了较好的效果。

2．我国的计算机信息安全立法

我国的计算机信息安全立法模式基本上属于“渗透型”，国家未制定统一的计算机信息安全法，而是将涉及信息安全的法律规范渗透和融入相关法律、行政法规、部门规章和地方法规中，初步形成了由不同法律效力层构成的计算机信息安全法律规范体系。

我国信息安全立法有 4 个层次：一是由全国人大常委会通过的法律，除警察法、刑法、保守国家秘密法外，涉及计算机信息安全的法律还有《全国人大常委会关于维护互联网安

全的决定》等；二是国务院为执行宪法和法律而制定的行政法规，主要有《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》和《互联网上网服务营业场所管理条例》等；三是国务院各部委根据法律和行政法规在本部门权限范围内制定的规章及规范性文件，主要有《计算机病毒防治管理办法》、《互联网电子公告服务管理规定》、《国际互联网出入信道管理办法》、《中国互联网络域名注册实施细则》、《互联网信息服务管理办法》等；四是各省市自治区制定的地方性法规，例如《××省计算机信息系统安全保护管理规定》等。

我国缔约或参加的有关计算机及网络信息的国际公约有《建立世界知识产权组织公约》、保护文化艺术作品的《伯尔尼公约》、《世界版权公约》、《与贸易有关的知识产权（包括假冒商品贸易）协议》等。

1.4.2　安全管理

各计算机网络使用机构、企业或单位，应建立相应的网络安全管理制度，加强内部管理，建立合适的网络安全管理系统，建立安全审计和跟踪机制，提高整体网络的安全性。

网络安全管理措施包括建立、健全安全管理机构、行政人事管理和系统安全管理制度等。

1. 安全管理机构

为保证计算机网络系统的安全运行，网络系统的使用单位应当成立计算机安全管理机构，设立专职安全人员。这些安全人员包括安全管理、安全审计、系统分析、软硬件管理、通信及保安人员等。

网络安全管理机构的设置与系统的规模直接相关。若是一个庞大系统且终端客户遍布世界各地，则在每个区域内都应有一个这样的管理机构。所以，一个网络系统设置多少安全管理机构是不定的，但机构中各有关方面人员的职责是固定的。

（1）安全管理机构的主要职责

① 统一规划网络系统的安全，制定完善的安全策略和措施，协调各方面的安全事宜等。

② 建立网络安全管理规章制度。

③ 选择和确定网络安全管理负责人和安全管理人员。

④ 明确职责，制定有关的责任追究制度。

（2）安全管理机构的组成人员及其职责

① 安全管理人员。安全管理人员具体负责本系统或本区域内安全策略的实施，保证安全策略的长期有效性，负责可信软/硬件的安装和维护、日常操作的监视、应急情况下安全措施的恢复和风险分析等。

② 安全审计人员。安全审计实际可归入安全管理，同样担负着保证系统安全的责任，其具体工作是监视系统的运行情况，收集对系统资源的各种非法访问事件并进行记录，然后进行分析处理，如有必要，还要将审计的事件及时上报主管领导。

③ 保安人员。保安人员主要负责非技术性的、常规的安全保卫工作，例如计算机网络系统场地的警卫、验证出入网络中心的手续和各种规章制度的落实等。

④ 系统管理人员。系统管理人员包括网络系统的软/硬件技术人员、系统分析和测试人员、通信管理与维护人员等。这些人员虽然不是直接负责系统的安全保卫工作，但仍是保证系统安全运行的重要组成部分。其主要工作是安装、调试和升级系统，控制系统操作，监视系统运行，维护和管理系统正常工作等。

⑤ 安全管理机构负责人。在安全管理机构中，负责人责任重大。他宏观负责整个系统的安全，其主要任务有对系统修改进行授权，对特权和口令进行授权，对每天的违章报告、控制室记录、系统工作审计记录等进行审阅，负责对安全人员组织培训，遇到重大问题向系统主管领导及时报告等。

2. 安全行政人事管理

对计算机网络信息系统的大部分威胁都来自人为因素，因为无论系统如何自动化，总是由人设计和操作使用的，而人本身是很复杂的，受自身生理和心理因素的影响和制约，有时为了达到某种目的而不惜铤而走险，利用计算机系统进行犯罪活动。据研究表明，从事计算机职业犯罪的人员中，70%是信息系统运行和管理人员。因此，对信息系统的运行和管理人员进行教育、奖惩、培养和训练，加强行政和人事管理，对保证网络信息安全是非常必要的。

行政人事管理的职责是：制定严格的人事管理、岗位分工、奖惩和责任追究等规章制度，使网络系统工作人员做到各司其职、各负其责、互相监督和制约，保证系统安全运行。行政人事管理的具体工作有以下一些内容：

（1）人事审查和录用

凡接触到机密信息的人员，必须坚持先审查后录用的原则。审查一般包括个人历史审查、人品审查、对在职人员的定期或不定期的审查等。录用时应挑选那些技术能力和道德素质好的人员管理和操作网络系统，确保这些人员的纯洁和可靠。此外，还应与被录用人员签署入职和保密协议。

（2）岗位和职责范围的确定

在网络系统中，一般需要安全管理、安全审计、系统管理、系统分析、系统工程、系统维护、系统操作、信息录入等人员。确定岗位之后，明确责任分工就成为安全管理的基础，所以要制定各类管理人员的职责范围，决不允许越权管理。这样就能使系统管理人员各司其职、互相制约，从而减少犯罪的可能性，达到安全的目的。

（3）工作考核和评价

定期对系统管理人员的政治思想、业务水平、工作表现等进行考核，对他们的成绩进行评价和表彰，激发他们的工作热情，同时依据评价和考核结果对他们进行必要的提升、调动和任免。

（4）任期有限原则

任何人不要在一个安全管理岗位上长期任职。

（5）最小权限原则

对任何安全管理人员，只授予其完成本职工作所需要的基本权限，分散超级用户的使

用权限。

（6）教育与培训

对刚被录用人员要先进行培训，培训内容包括职业道德、安全教育、法制教育、在工作岗位上可能遇到的新技术或新工作方法、各种操作规程等，经考核合格者核发相关上岗证件，杜绝无证上岗现象。对已录用的人员也要定期进行培训，以提高其工作水平。

（7）人事档案管理

建立相关制度，限制无关人员接触人事档案。一旦工作人员的岗位和职责发生变化，要及时在档案内补充材料，以确保档案反映工作人员的工作和生活实情。

3. 系统安全管理

一般来说，网络系统的安全管理主要是确定安全管理原则和相应的安全管理制度。网络系统安全管理机构应根据多人负责制、职责分离、任期有限和最小权限等原则，制定相应的管理制度或规范。

（1）确定安全等级

确定网络系统的安全等级；根据系统的安全等级，确定系统的安全管理范围。对安全等级要求较高的系统，要进行分区控制，限制工作人员出入无关的区域。人员的出入管理可采用身份证件识别，或安装自动识别登记系统，例如采用磁卡、身份卡等手段对出入人员进行识别和登记。

（2）制定管理制度

制定计算机机房安全管理制度、机房设备和数据管理制度。其内容可包括：保持机房整洁卫生，不得在机房内吸烟、吃东西；非机房工作人员不得擅自进入机房；上机人员在指定的计算机上工作，禁止做与工作无关的事情，如玩电子游戏；建立工作手册和工作记录，对每月计算机信息系统的运行状况、故障原因、维修处理结果、业务进行详细记录；数据输入应验证其准确性，数据修改时应保证数据的一致性和完整性，重要数据由专人输入，重要数据的修改需经主管领导批准并有领导在场；重要数据的打印输出及外存介质应放在安全的地方，打印出的废纸要及时销毁，外存的数据要进行加密处理，损坏的外存介质要及时粉碎报废。

（3）对操作系统和数据库的访问要有监控措施，访问权限应按工作性质划分

不得将系统特权授予普通用户，不得将所授予的特权转让给其他用户，必要时要收回授予的特权并修改特权程序。

（4）制定严格的操作规程

操作规程也要根据多人负责和职责分离的原则进行，不得越权操作和代替别人操作。如进行程序开发时，应指定运行程序和修改程序的人员，并将运行和修改程序的人员分开。

（5）安全审计跟踪

网络系统运行时要有安全审计跟踪措施，能随时掌握网络用户的工作情况。

（6）备份

有用的数据和程序要及时备份，妥善保管，重要的数据和程序由专人备份和保管，必

要时备份两份并异地保存。

（7）制定完备的系统维护制度

内容包括对系统进行维护时应采取的数据保护措施；维护时要先经管理部门批准，并有安全管理人员在场；对维护的部位、故障原因、维护内容和维护前后的情况进行详细记录。

（8）制定计算机网络系统的灾害处理对策、灾难恢复计划和具体恢复措施

制定应急措施，在紧急情况下，要尽快恢复系统，使损失降到最低程度。

（9）制定人员调离安全制度

人员调离前应移交系统的所有文档资料，及时更换系统口令，对调离人员重申离岗后承担的安全与保密的责任和义务。

1.4.3　实体安全技术和访问控制技术

1. 实体安全技术

网络实体安全（物理安全）保护就是指采取一定措施对网络的硬件系统、数据和软件系统等实体进行保护和对自然与人为灾害进行防御。

对网络硬件的安全保护包括对网络机房和环境的安全保护、网络设备设施（例如，通信电缆等）的安全保护、信息存储介质的安全保护和电磁辐射的安全保护等。

对网络数据和软件的安全保护包括对网络操作系统、网络应用软件和网络数据库数据的安全保护。

对自然与人为灾害的防御包括对网络系统环境采取防火、防水、防雷电、防电磁干扰、防振动以及防风暴、防地震等措施。

2. 访问控制技术

访问控制就是规定哪些用户可访问网络系统，对要求入网的用户进行身份验证和确认，这些用户能访问系统的哪些资源，他们对于这些资源能使用到什么程度等。访问控制的基本任务就是保证网络系统中所有的访问操作都是经过认可的、合法的，防止非法用户进入网络和合法用户对网络系统资源的非授权访问。

访问控制措施通常包括设置口令和入网限制，如采用 CA 认证、数字证书、数字签名等技术对用户身份进行验证和确认，规定不同软件及数据资源的属性和访问权限，进行网络监视，设置网络审计和跟踪，使用防火墙系统、入侵检测和防护系统等。

1.5　信息安全评价标准

计算机信息系统安全产品种类繁多，功能也各不相同，为了更好地对其安全性进行客观评价，满足用户对安全功能和保护措施的多种需求，也便于同类安全产品进行比较，许

多国家都分别制定了各自的信息安全评价标准。典型的信息安全评价标准主要有美国国防部颁布的《可信计算机系统评价标准》；欧洲的德国、法国、英国、荷兰 4 国联合颁布的《信息技术安全评价标准》；加拿大颁布的《可信计算机产品评价标准》；中国国家质量技术监督局颁布的《计算机信息系统安全保护等级划分准则》。

1.5.1　美国《可信计算机系统评价标准》

1985 年，美国国防部基于军事计算机系统保密工作的需求，在历史上首次颁布了《可信计算机系统评价标准》（Trusted Computer System Evaluation Criteria，TCSEC），把计算机安全等级分为 4 类 7 级（按照安全从低到高的级别顺序，依次为 D、C1、C2、B1、B2、B3、A 级），如表 1-1 所示。

表 1-1　TCSEC

级　别	名　称	特　征
A	验证设计安全级	形式化的最高级描述和验证，形式化的隐蔽通道分析，非形式化的代码一致性证明
B3	安全域级	安全内核，高抗渗透能力
B2	结构化安全保护级	面向安全的体系结构，遵循最小授权原则，有较好的抗渗透能力，对所有的主体和客体提供访问控制保护，对系统进行隐蔽通道分析
B1	标记安全保护级	在 C2 安全级上增加了安全策略模型，数据标记（安全和属性），托管访问控制
C2	访问控制环境保护级	访问控制，以用户为单位进行广泛的审计
C1	选择性安全保护级	有选择的访问控制，用户与数据分离，数据以用户组为单位进行保护
D	最低安全保护级	保护措施很少，没有安全功能

这些等级的内涵如下：

（1）D 级为最低安全保护级。该级不设任何安全保护措施，软硬件都容易被侵袭，MS-DOS、Windows 95/98 等系统属于这个级别。

（2）C1 级是选择性安全保护级。C1 级对硬件采取简单的安全措施，例如加锁，用户要有登录认证和访问权限制，但不能控制已登录用户的访问级别，早期的 UNIX/Xenix、Netware 3·x 及以下版本系统均属于该级别。

（3）C2 级是访问控制环境保护级。C2 级比 C1 级增加了几个特性，例如系统审计、跟踪记录、安全时间等。UNIX/Xenix、Netware 3·x 级以上版本、Windows NT 等系统属于本级。该级也是保证敏感信息安全的最低级。

（4）B1 级是标准安全保护级。B1 级的系统安全措施支持多级（网络、应用程序和工作站等）安全。标记（Label）是指网上的一个对象，该对象在安全保护计划中是可识别且受保护的。该级别是支持秘密、绝密信息保护的第一个级别。B1 级系统拥有者主要为政府机构和防御承包商。

（5）B2 级是结构化安全保护级。B2 级要求系统中所有对象都加标记，并给各设备分配安全级别。例如，允许用户访问一工作站，却不允许访问含有特定资料的磁盘子系统。

（6）B3 级是安全域级。B3 级要求用户工作站或终端通过可信任途径连接网络系统。该级还采用硬件来保护安全系统的存储区。

（7）A 级是验证设计安全级。A 级是最高安全级，包含了低级别所有的特性。A 级包括一个严格的设计、控制和验证过程，设计必须是从数学角度经过验证的，且必须进行隐蔽通道和可信任分析。

1.5.2 其他国家信息安全评价标准

1. 德国《计算机安全评价标准》

德国信息安全部颁布的《计算机安全评价标准》绿皮书在 TCSEC 的基础上增加了系统有效性和数据完整性要求，共定义了 10 个安全功能类别和 8 个实现安全功能的质量保障等级，安全功能类别用 F1～F10 表示，安全质量保障等级用 Q0～Q7 表示。其中 F1～F5 分别对应 TCSEC 的 C1～B3 安全等级，F6、F7 是针对数据完整性定义的安全功能需求，F8～F10 是针对数据通信环境定义的安全需求。Q0～Q7 安全质量保障等级大致对应 TCSED 的 D～A 和超 A 保障能力，超 A 是 TCSEC 为适应安全技术发展预留的评价标准，没有制定详细的评价规范。

2. 德、法、英、荷 4 国联合制定的《信息技术安全评价标准》

欧洲共同体成员国德国、法国、英国、荷兰联合制定的《信息技术安全评价标准》（ITSEC）在吸收 TCSEC、英国标准和德国绿皮书经验的基础上，首次提出了信息保密性、完整性和有效性安全目标概念。在保留德国绿皮书 10 个安全功能 F1～F10 和英国标准功能描述语言的同时，ITSEC 定义了 7 个安全功能可信等级 E0～E6（称为有效性等级），分别对应 TCSEC 的 D～A 安全等级。

3. 加拿大《可信计算机产品评价标准》

加拿大制定的《可信计算机产品评价标准》（Canadian Trusted Computer Product Evaluation Criteria，CTCPEC）也将产品的安全要求分成安全功能和功能保障可依赖性两个方面。其中，安全功能根据系统保密性、完整性、有效性和可计算性定义了 6 个不同等级 0～5。保密性包括隐蔽信道、自主保密和强制保密；完整性包括自主完整性、强制完整性、物理完整性和区域完整性等属性；有效性包括容错、灾难恢复及坚固性等；可计算性包括审计跟踪、身份认证和安全验证等属性。根据系统结构、开发环境、操作环境、说明文档及测试验证等要求，CTCPEC 将可依赖性定为 8 个不同等级 T0～T7，其中 T0 级别最低，T7 级别最高。德国绿皮书标准、ITSEC 标准、CTCPEC 标准与 TCSEC 标准之间的大致对应关系，如表 1-2 所示。

表 1-2　安全评价标准之间的大致对应关系

德国绿皮书标准		ITSEC 标准		CTCPEC 标准		TCSEC 标准
功能等级	可信等级	功能等级	可信等级	功能等级	可信等级	安全等级
	Q0		E0		T0	D
F1	Q1	F1	E1		T1	C1
F2	Q2	F2	E2	0	T2	C2
F3	Q3	F3	E3	1	T3	B1
F4	Q4	F4	E4	2	T4	B2
F5	Q5	F5	E5	3	T5	B3
	Q6	F6	E6	4	T6	A
	Q7			5	T7	超 A

1.5.3　我国信息安全评价标准

由于信息安全直接涉及国家政治、军事、经济和意识形态等许多重要领域，各国政府对信息系统或技术产品安全性的测评认证要比其他产品更为重视。尽管许多国家签署了《信息技术安全评价公共标准》(Common Criteria for Information Technology Security Evaluation，CC)，但很难想象一个国家会绝对信任其他国家对涉及国家安全和经济的产品的测评认证。事实上，各国政府都通过颁布相关法律、法规和技术评价标准对信息安全产品的研制、生产、销售、使用和进出口进行了强制管理。

中国国家质量技术监督局1999年颁布的《计算机信息系统安全保护等级划分准则》(GB 17859—1999)，在参考 TCSEC、ITSEC 和 CTCPEC 等标准的基础上，将计算机信息系统安全保护能力划分为用户自主保护、系统审计保护、安全标记保护、结构化保护、访问验证保护 5 个安全等级，分别对应 TCSEC 标准的 C1～B3 等级。为了与国际通用安全评价标准接轨，国家质量技术监督局于 2001 年 3 月又正式颁布了国家推荐标准《信息技术—安全技术—信息技术安全性评估准则》(GB/T 18336—2001)，推荐标准完全等同于国际标准 ISO/IEC 15408，即《信息技术安全评价公共标准》第 2 版。

推荐标准 GB/T 18336—2001 由 3 部分组成：第一部分是《简介和一般模型》(GB/T 18336.1)，第二部分是《安全功能要求》(GB/T 18336.2)，第三部分是《安全保证要求》(GB/T 18336.3)，分别对应国际标准化组织和国际电工委员会国际标准 ISO/IEC 15408-1、ISO/IEC 15408-2 和 ISO/IEC 15408-3。

《信息技术安全评价公共标准》、《计算机信息系统安全保护等级划分准则》(GB 17859—1999)、《信息技术安全性评估准则》(GB/T 18336—2001）与美国 TCSEC 标准的对应关系如表 1-3 所示。

表 1-3　CC 及国家标准与 TCSEC 标准的对应关系

CC 标准	国家标准 GB 17859—1999	国家推荐标准 GB/T18336—2001	TCSEC 标准
			D
EAL1		EAL1	
EAL2	用户自主保护	EAL2	C1
EAL3	系统审计保护	EAL3	C2
EAL4	安全标记保护	EAL4	B1
EAL5	结构化保护	EAL5	B2
EAL6	访问验证保护	EAL6	B3
EAL7		EAL7	A

小　　结

网络安全就是为防范计算机网络硬件、软件、数据偶然或蓄意被破坏、篡改、窃听、假冒、泄露、非法访问并保护网络系统持续有效工作的措施总和。

网络安全的最终目标就是通过各种技术与管理手段实现网络系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性，通常更侧重强调网络信息的保密性、完整性和有效性。

网络安全的特征表现在系统的可靠性、软件和数据的完整性、可用性和保密性等几个方面。

网络安全策略是保障机构网络安全的指导文件，包括总体安全策略和具体安全管理实施细则。安全策略的总则：均衡性原则、时效性原则、最小限度原则。安全内容有：网络硬件物理安全、网络连接安全、操作系统安全、网络服务安全、数据安全、安全管理责任、安全用户责任。

网络安全设备、网络安全增强和针对性防范技术既是经典网络安全技术的直接延伸，也是下一代网络安全技术的基础，而网络安全管理是下一代网络安全技术的核心。

网络安全漏洞包括：软件漏洞、网络协议漏洞和安全管理漏洞。软件漏洞是指在软件设计与编制时没有考虑非正常输入处理或错误代码造成的安全隐患，也称为软件脆弱性或软件隐错。

网络系统的威胁大致可分为无意威胁和故意威胁两大类。无意威胁是在无预谋的情况下破坏系统的安全性、可靠性或信息的完整性等；故意威胁实际上就是“人为攻击”。

一个网络安全模型通常由信息转换的收发双方、可信任的第三方以及传输链路上受攻击方组成。

网络信息安全框架由 OSI 安全层次、安全特性和系统单元组成三维空间。OSI 安全层次涵盖了 OSI 体系结构提出的从物理层到应用层的层次，其中不包含会话层和表示层；安全特性是指该安全单位可以解决哪些安全威胁；系统单元是指该安全单元解决什么系统环

境的问题。

OSI 网络安全体系结构主要包括网络安全机制和网络安全服务两方面的内容。网络安全机制包含加密机制、数字签名机制、访问控制机制、数据完整性机制、交换鉴别机制、信息流填充机制、路由控制机制和公证机制等；网络安全服务有鉴别服务、访问控制服务、数据完整性服务、数据保密性服务和非否认服务等。

P2DR 网络安全模型由相互关联的策略、保护、检测和响应 4 部分组成，安全策略是 P2DR 模型的核心。

计算机犯罪是一种高技术犯罪活动，也是未来社会的主要犯罪形式之一，面对其日益严重的威胁，必须建立、健全相关的法律、法规进行约束。我国和其他国家都进行了计算机信息安全立法，设立专门的机构和人员进行这项管理工作。

网络实体安全保护就是指采取一定措施对网络的硬件系统、软件系统和数据等实体进行保护和对自然和人为灾害进行防御；访问控制就是规定哪些用户可访问网络系统，对要求入网的用户进行身份验证和确认，规定其能访问系统哪些资源，对这些资源可使用到什么程度等问题。

美国提出的《可信计算机系统评价标准》（TCSEC），将安全级别分为 D、C、B、A 四大类，安全级别按 D、C1、C2、B1、B2、B3、A 依次增高，安全风险依次降低，高安全级别的计算机系统包含了低安全级别的属性。

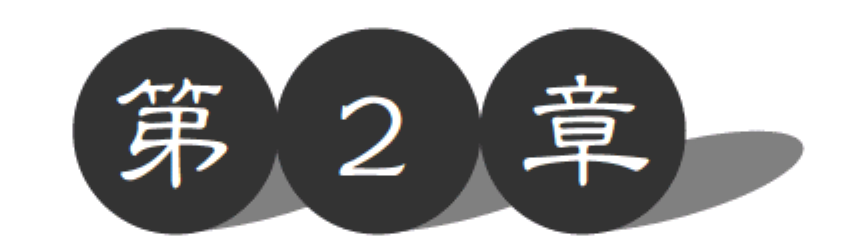
德国《计算机安全评价标准》绿皮书定义了 10 个安全功能类别和 8 个实现安全功能的质量保障等级，安全功能类别用 F1～F10 表示，安全质量保障等级用 Q0～Q7 表示。欧洲共同体成员国德、法、英、荷 4 国联合制定的 ITSEC 定义了 10 个安全功能类 F1～F10 和安全功能可信等级 E0～E6。加拿大的 CTCPEC 定义了 6 个不同等级 0～5 和 8 个可依赖性等级 T0～T7。

目前我国有两个信息安全评价标准，分别是国家标准《计算机信息系统安全保护等级划分准则》（GB 17859—1999）和国家推荐标准《信息技术—安全技术—信息技术安全性评估准则》（GB/T 18336—2001）。GB 17859—1999 将信息系统安全保护能力划分为 5 个安全等级，GB/T 18336—2001 等同于国际标准 ISO/IEC15408。目前我国信息安全测评认证中心采用 GB/T 18336—2001 对国内外信息安全产品和信息技术进行测评和认证。

练习与思考

1. 什么叫计算机网络安全？计算机系统安全与密码的关系是什么？
2. 网络安全的目标是什么？简述保密性、完整性和有效性的含义，分别使用什么技术手段能够保障网络信息的保密性、完整性和有效性？
3. 网络安全策略的具体内容有哪些？
4. 什么叫软件漏洞？什么叫网络协议漏洞？请列举一些网络事例予以说明。
5. 网络系统的威胁有哪些类别？它们的内涵分别是什么？

6．为什么软件漏洞具有时效性特点？
7．网络安全模型由哪几部分组成？一个安全的网络通信方案必须考虑哪些内容？
8．网络信息安全框架是一个几维空间？其中的系统单位涉及哪些不同环境？
9．P2DR 网络安全模型由哪几部分组成？请说明各部分的作用。
10．为什么要进行计算机信息安全立法？我国信息安全立法从哪 4 个层次考虑？
11．简述美国《可信计算机系统评价标准》D、C、B、A 四大类安全级别的安全属性。
12．我国颁布的《计算机信息系统安全保护等级划分准则》建立在什么基础上？



数据加密技术

本章学习要求：

（1）掌握数据加密的基本概念。
（2）掌握传统的密码技术。
（3）掌握对称密钥密码和公开密钥密码体制。
（4）掌握密钥管理。
（5）掌握数字签名的方法。
（6）了解加密软件 PGP 提供的服务。
（7）了解网络保密通信。

重点和难点：

（1）重点：掌握数据加密的基本概念、对称密钥密码和公开密钥密码体制。
（2）难点：掌握数字签名的方法。

尽管采用安全立法对保护网络系统安全有着不可替代的重要作用，但任何法律也阻止不了攻击者对网络数据的各种威胁；加强行政、人事管理，采取物理保护措施都是保护系统不可缺少的有效措施，但是这些措施也会受到各种环境、费用、技术以及系统工作人员素质等条件的限制；采用访问控制、系统软硬件保护等方法保护网络系统资源，简单易行，但也存在像系统内部某些职员可以轻松越过这些障碍而进行计算机犯罪等不易解决的问题；而采用密码技术和数据加密技术保护网络中存储和传输的数据，则是一种十分实用、经济、有效的方法。对数据信息进行加密保护可以防止攻击者窃取网络机密信息，使系统信息不被非法者识别，也可以检测出非法用户对数据的插入、删除和修改及滥用有效数据等各种行为。

本章将讨论数据加密概述、传统的密码技术、对称密钥和公开密钥密码体制、数字签名、密钥管理、网络保密通信和加密软件 PGP。

2.1 数据加密概述

2.1.1 密码学的发展

密码学（Cryptography，来源于古希腊的 Crypto 和 Graphein，意思是密写）是一门古老而深奥的学科，它以认识密码变换为本质，以加密与解密基本规律为研究对象。一般人对密码学是陌生的，因为长期以来，它只被应用在军事、外交和情报等部门。

早在几千年前，人类就已经有了保密通信的思想和方法，但这些保密方法都是非常朴素、原始和低级的，而且大多数是无规律的。有记载的最早的密码系统可能是希腊历史学家发明的 Polybios，这是一种替代密码系统。

1949 年，信息论的创始人香农（C. E. Shannon）发表了一篇著名的文章，论证了一般经典加密方法都是可以破解的。到了 20 世纪 60 年代，随着电子技术、信息技术的发展及结构代数、可计算性理论和复杂度理论的研究，密码学又进入了一个新的时期。

近年来，密码学研究之所以十分活跃，主要是它与计算机科学的蓬勃发展密切相关；此外，还有在电信、金融等领域防止日益泛滥的计算机犯罪的需要。在互联网出现之前，密码技术已经广泛应用于军事和民用方面，而今密码技术应用于计算机网络中的实例越来越多。

密码学的发展可分为两个主要阶段：第一个阶段是传统密码学阶段，即古代密码学阶段，该阶段基本上依靠人工和机械对信息进行加密、传输和破译；第二阶段是计算机密码学阶段，该阶段又可细分为两个阶段，即使用传统方法的计算机密码学阶段和使用现代方法的计算机密码学阶段。使用传统方法的计算机密码学是指计算机密码工作者沿用传统密码学的基本观念进行信息的保密；而使用现代方法的计算机密码学是指使用现代思想进行信息的保密，其中包括两个方向，即对称密钥密码机制和非对称密钥密码机制。

计算机密码学是研究利用现代技术手段对计算机系统中的数据进行加密、解密和变换的学科，是数学和计算机学交叉的学科，也是一门新兴的学科。随着计算机网络和现代通信技术的发展，计算机密码学得到了前所未有的发展和应用。在国外，计算机密码学已成为计算机系统安全的主要研究方向，也是计算机安全课程教学中的主要内容。

密码学包括密码编码学和密码分析学。密码编码学是研究密码变化的规律并用之于编制密码以保护秘密信息的科学，即研究如何通过编码技术来改变被保护信息的形式，使得编码后的信息除指定接收者之外的其他人都不能理解；密码分析学则是研究密码变化的规律并用之于分析（解释）密码以获取信息情报的科学，即研究如何攻破一个密码系统，恢复被隐藏起来的信息的本来面目。密码编码学是实现对信息加密的，密码分析学是实现对信息解密的，这两部分相辅相成，互相促进，也是矛盾的两个方面。

在 20 世纪 70 年代，密码学的研究出现了两大成果，一个是 1977 年美国国家标准局（NBS）颁布的联邦数据加密标准（DES），另一个是 1976 年由 Diffie 和 Hellman 提出的公

钥密码体制的新概念。DES 将传统的密码学发展到了一个新的高度，而公钥密码体制的提出被公认为是实现现代密码学的基石。这两大成果已成为近代密码学发展史上的两个重要里程碑。

随着计算机网络不断渗透到国民经济各个领域，密码学的应用也随之扩大，数字签名、身份鉴别等都是由密码学派生出来的新技术和新应用。

2.1.2　密码学的基本概念

在计算机网络系统中，可采用密码技术将信息隐蔽起来，再将隐蔽后的信息进行存储和传输。这样，即使信息在存储或传输过程中被窃取或截获，那些非法获得信息者因不了解这些信息的隐蔽规律，也就无法识别信息的内容，从而保证了计算机网络系统中的信息安全。

在密码学中，通过使用某种算法并使用一种专门信息——密钥，可将信息从一个可理解的明码形式变换成一个错乱的不可理解的密码形式，只有再使用密钥和相应的算法才能把密码还原成明码。

1．密码学的基本术语

（1）消息（Message）

消息是指用语言、文字、数字、符号、图像、声音或其组合等方式记载或传递的有意义的内容。在密码学里，消息也称为信息。

（2）明文（Plaintext）

未经过任何伪装或隐藏技术处理的消息称为明文。

（3）加密（Encryption）

利用某些方法或技术对明文进行伪装或隐藏的过程称为加密。

（4）密文（Cipher Text）

被加密的消息称为密文。

（5）解密（Decryption）

将密文恢复成原明文的过程或操作称为解密。解密也可称为脱密。

（6）加密算法（Encryption Algorithm）

将明文消息加密成密文所采用的一组规则或数学函数。

（7）解密算法（Decryption Algorithm）

将密文消息解密成明文所采用的一组规则或数学函数。

（8）密钥（Key）

进行加密或解密操作所需要的秘密参数或关键信息。在密码系统中，密钥分为私钥与公钥两种。私钥指必须保密的密钥，公钥指可以向外界公开的密钥。

（9）密码体制（Cryptosystem）

一个密码体制或密码系统是指由明文空间、密文空间、密钥空间、加密算法以及解密算法组成的一个多元素集合体。对任何一个密码体制（系统）来说，决定其安全性的重要

参数是密钥，而非算法。算法一般是公开的。

2．加解密过程

通用的数据加密模型如图 2-1 所示。

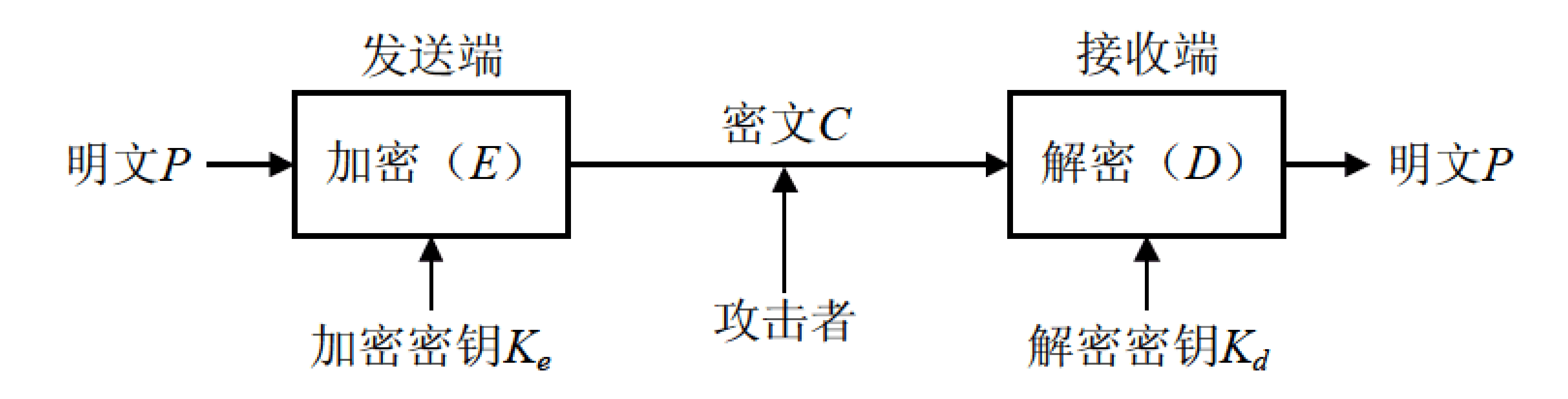


图 2-1　通用的数据加密模型

从图 2-1 可见，加密算法实际上是要完成其函数 $c=f(P, K_e)$的运算。对于一个确定的加密密钥 K_e，加密过程可看作是只有一个自变量的函数，记作 E_k，称为加密变换。因此加密过程也可记为：

$$C=E_k(P)$$

即加密变换作用到明文 P 后得到密文 C。

同样，解密算法也是完成某种函数 $P=g(K_d, C)$的运算，对于一个确定的解密密钥 K_d 来说，解密过程可记为：

$$P=D_k(C)$$

其中，D_k 称为解密变换，D_k 作用于密文 C 后得到明文 P。

由此可见，密文 C 经解密后还原成原来的明文，必须有：

$$P=D_k(E_k(P))=D_k \cdot E_k(P)$$

此处“•”是复合运算，因此要求：

$$D_k \cdot E_k=I$$

在此 I 为恒等变换，表明 D_k 与 E_k 是互逆变换。

2.1.3 密码的分类

从不同的角度，根据不同的标准，可将密码分为不同的类型。

1．手工密码、机械密码、电子机内乱密码和计算机密码

按密码的历史发展阶段和应用技术划分，可将其分为手工密码、机械密码、电子机内乱密码和计算机密码。

（1）手工密码是以手工完成，或以简单器具辅助完成加密和解密过程的密码。这是第一次世界大战以前使用的主要密码形式。

（2）机械密码是以机械密码机或电动密码机来实现加密和解密过程的密码。这种密码最早出现在第一次世界大战期间，在第二次世界大战中得到普遍应用。

（3）通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产大量的加密乱

数，因其制乱是在加密、解密过程中完成的而不需预先制作，所以称为电子机内乱密码。

（4）计算机密码是指以计算机软件程序完成加密和解密过程的密码，适用于计算机数据保护和网络保密通信场合。

2. 替代密码和移位密码

按密码转换操作的原理划分，可将密码分为替代密码和移位密码。

（1）替代密码也叫置换密码，就是在加密时将明文中的每个或每组字符由另一个或另一组字符替换，原字符被隐藏起来，即形成密文。

（2）移位密码也叫换位密码，就是在加密时只对明文字母（字符、符号）重新排序，每个字母位置变化了，但没被隐藏起来。移位密码是一种打乱原文顺序的加密方法。

替代密码加密过程是明文的字母位置不变而字母形式变化了，移位密码加密过程是字母的形式不变而位置变化了。

3. 保密密码和不保密密码

按保密程度划分，可将密码分为理论上保密的密码、实际上保密的密码和不保密的密码。

（1）理论上保密的密码是指不管获取多少密文和有多大的计算能力，始终不能破译原信息，这种密码也叫理论不可破译的密码。

（2）实际上保密的密码是指在理论上可破译，但在现有客观条件下，无法通过计算来得到原信息，或即使破译成功，得到了原信息，但此时原信息早已过了实效期而没有任何意义了。

（3）不保密的密码是指在获取一定数量的密文后，使用一些技术即可得到仍有意义的原信息。例如，早期单表代替密码、后来的多表代替密码等至今都已成为不保密的密码。

4. 分组密码和序列密码

按明文加密时的处理过程划分，可将密码分为分组密码和序列密码。

（1）分组密码

分组密码的加密过程是：首先将明文序列以固定长度进行分组（数据块），每组明文用相同的密钥和算法进行变换，得到一组密文。分组密码是以分组为单位，在密钥的控制下进行一系列线性和非线性变换而得到密文的。

在分组密码的加密/解密运算过程中，输出块中的每一位是由输入块的每一位和密钥的每一位共同决定的。加密算法中重复地使用替代和移位两种基本的加密变换，此即 Shannon 于 1949 年发现的隐藏信息的两种技术——扩散和扰乱。

① 扩散（Diffusion）就是把明文的统计结构扩散消失到密文的长度统计特性中。其方法是使明文的每个数字影响许多密文数字的取值，即每个密文数字被许多明文数字影响。其结果是在密文中各种字母出现的频率比在明文中更接近平均，双字母组合出现的频率也更接近平均。所有分组密码都包含从明文分组到密文分组的变换，具体变换依赖于密钥。扩散机制使得明文和密文之间的统计规律尽量复杂，以便增大推测密钥的难度。

② 扰乱（Conffusion）即试图使密文的统计特性与加密密钥取值之间的关系尽量复杂，同样也是为了增大发现密钥的难度。这样，即使攻击者掌握了密文的某些统计特性，由于密钥产生密文的方式非常复杂，攻击者也难于从中推测出密钥。要实现这个目的，可使用一个复杂的替代算法。

分组密码具有良好的扩散性、对插入信息的敏感性、较强的适应性、加密/解密速度慢、差错的扩散和传播等特点。

（2）序列密码

序列密码的加/解密过程是：把报文、语音、图像等原始信息转换为明文数据序列，再将其与密钥序列进行“异或”运算，生成密文序列发送给接收者；接收者用相同的密钥序列与密文序列再进行逐位解密（异或），恢复明文序列。序列密码加密/解密的密钥，可采用一个比特流发生器随机产生二进制比特流而得到。这些随机比特流作为密钥，与明文结合产生密文，与密文结合产生明文。序列密码的安全性主要依赖于随机密钥序列。

5．对称密钥密码和非对称密钥密码

按加密和解密密钥的类型划分，可将密码分为对称密钥密码和非对称密钥密码。

加密和解密过程都是在密钥的作用下进行的。如果加密密钥和解密密钥相同或相近，由其中一个很容易地得出另一个，这样的系统称为对称密钥密码系统。在这种系统中，加密和解密密钥都需要保密。对称密钥密码系统也称为单密钥密码系统或传统密钥密码系统。

如果加密密钥与解密密钥不同，且由其中一个不容易得到另一个，则这种密码系统是非对称密钥密码系统。这两个不同的密钥，往往其中一个是公开的，另一个是保密的。非对称密钥密码系统也称为双密钥密码系统或公开密钥密码系统。

2.2 传统密码技术

2.2.1 数据的表示

数据的表示有多种形式，使用最多的是文字，其次还有图形、声音、图像等。传统加密技术的主要对象是文字书信，其内容都是基于某个字母表，如英文字母表、汉语拼音字母表等。

现代密码技术是在计算机科学和数学基础上发展起来的，数据的各种表示形式在计算机系统中都是以某种编码方式存储的，而数据加密就是以这些数字化的信息为研究对象，所以现代密码技术可以应用于所有在计算机系统中运用的数据。计算机系统普遍采用的是二进制数据，所以二进制数据的加密方法在计算机系统信息安全中有着广泛的应用，它也是现代密码学研究的主要应用对象。

传统加密方法加密的对象是文字信息。文字由字母表中的字母组成，在字母表中字母是按顺序排列的，可赋予它们相应的数字序号，如表 2-1 所示。因为大多数加密算法都有

数学属性，这种表示方法便于对字母进行算术运算，因此可用数学方法进行加密变换。将字母表中的字母看作是循环的，将字母的加减运算变换为相应代码的算术运算，可用求模运算来表示（在标准的英文字母表中，模数为 26），如 A+4=E，X−10=H。

这是因为：

- l+4=5　　　　5mod 26=5　序号 5 对应的字母为“E”。
- 24+10=34　　34mod 26=8　序号 8 对应的字母为“H”。

表 2-1　英文字母表及其序号

字　母	代　码	字　母	代　码
A	1	N	14
B	2	O	15
C	3	P	16
D	4	Q	17
E	5	R	18
F	6	S	19
G	7	T	20
H	8	U	21
I	9	V	22
J	10	W	23
K	11	X	24
L	12	Y	25
M	13	Z	26

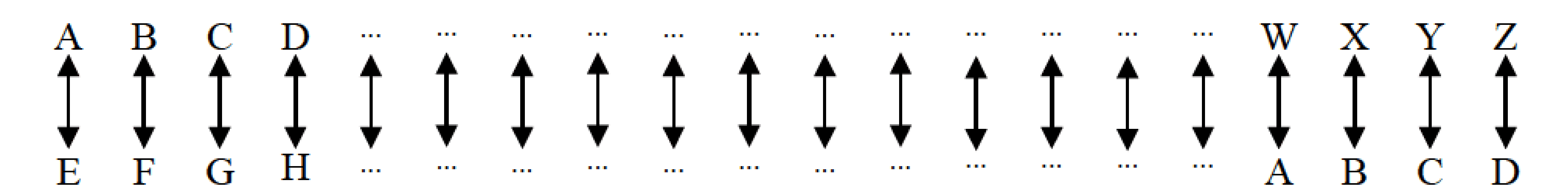
2.2.2　替代密码

替代密码在加密时将一个字母或一组字母的明文用另一个字母或一组字母替代，而得到密文；解密就是对密文进行逆替代得到明文的过程。

在传统密码学中，替代密码有简单替代、多名码替代、多字母替代和多表替代 4 种类型。

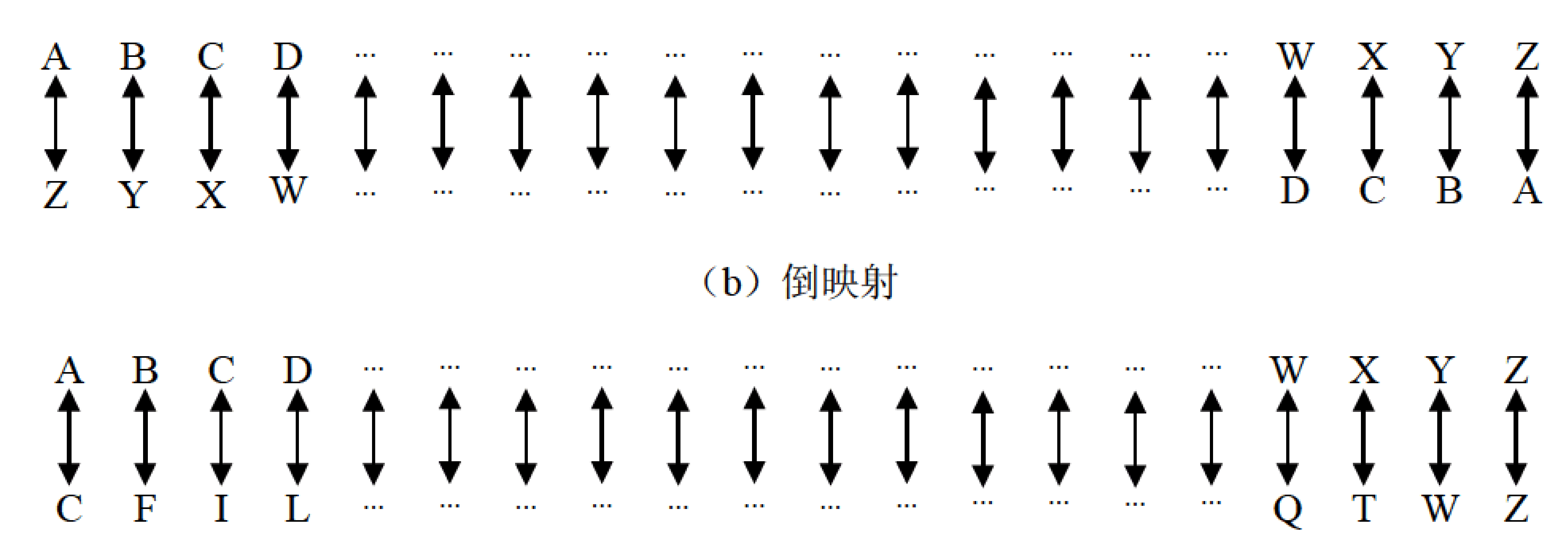
1. 简单替代密码

简单替代密码也叫单表替代密码。简单替代就是将明文的一个字母，用相应的一个密文字母代替；其规则是根据密钥形成一个新的字母表，与原明文字母表有相应的对应（映射）关系。简单替代加密方法有移位映射法、倒映射法和步长映射法等，如图 2-2 所示。



（a）移位映射

图 2-2　简单替代加密示意图



（b）倒映射

（c）步长映射（步长为 3）

图 2-2　简单替代加密示意图（续）

例如，移位映射的移动距离为+4（按字母顺序向右移动 4 个字母位置），则明文 A、B、C、…、Y、Z 可分别由 E、F、G、…、C、D 代替。如果明文是 about，则变为密文就是 efsyx，其密钥 k=+4，如图 2-2（a）所示。

简单替代密码很容易破译，因为它没有把明文不同字母出现的频率隐藏起来，所有密文都是由 26 个英文字母组成，字母出现的统计规律不变。破译这种密码的算法已经有很多种。

2. 多名码替代密码

多名码替代密码与简单替代密码的替代规则相似，不同之处是单个明文字母可以映射成几个密文字母，如 A 可能对应于 5、13、25 或 56，B 可能对应于 7、19、31 或 42 等。

多名码替代密码出现在 15 世纪初，虽然它比简单替代密码更难破译，但仍不能掩盖明文字母的统计特性。用已知明文攻击法破译该类密码很容易；用唯密文攻击法则要难一些，但在计算机上运行设计好的解密程序，只需要几秒钟即可完成破译。

3. 多字母替代密码

多字母替代密码的加密和解密都是将字母以块为单位进行的。比如，ABA 对应于 OST，ABB 对应于 STL 等。

多字母替代密码是在 19 世纪中期发明的，在第一次世界大战中，英国人就采用了这种对成组字母加密的密码。

4. 多表替代密码

多表替代密码是由多个简单替代密码构成的。一种常用的多表替代密码名为 Vigenere（维吉尼亚）密码，通过循环使用有限个字母实现了替代。Vigenere 密码是把 26 个字母循环移位，排列在一起，形成 26×26 的方阵表，加密和解密时的明文、密钥、密文就是表中的行、列及交点的内容。

多表替代密码有多个单字母密钥，每个密钥被用来加密一个明文字母。第一个密钥加密明文的第一个字母，第二个密钥加密明文的第二个字母，依此类推。在所有密钥用完后，密钥再被循环使用。若有 20 个密钥，那么每隔 20 个字母的明文都会被同一个密钥加密，

20 就是密码的周期，周期越长的密码越难破译，不过使用计算机可轻易地破译具有较长周期的替代密码。多表替代密码是 19 世纪后期发明的，曾在美国南北战争期间被联军使用过。

2.2.3　移位密码

移位密码加密时只对明文字母重新排序，字母位置变化了，但它们没有被隐藏。移位密码加密是一种打乱原文顺序的替代法。

例如，把明文 this is a bookmark 按行写出，分为 3 行、5 列，则成为以下形式。

t　h　i　s　i

s　a　b　o　o

k　m　a　r　k

读出时按从左到右的列顺序进行，可得到密文 tskhamibasoriok。则它的密钥就是 12345，即按列读出的顺序。

此外，还可以用另一种顺序选择相应的列输出得到密文。如用 china 为密钥，将 this is a bookmark 排列成上述矩阵，密钥 china 对应的序号为 23451。再以从小到大的顺序输出，即可得到密文 ioktskhamibasot。

又例如，对于句子“移位密码加密时只对明文字母重新排序字母位置变化但它们没被隐藏”，可选择密钥 362415，并循环使用该密钥对上句进行换位加密。密钥的数字序列代表明文字符（汉字）在密文中的排列顺序。按照该密钥加密可得到一个不可理解的新句子（密文）“密密位码移加对字只明时文新字重排母序置但位变母化没藏们被它隐”。解密时只需按密钥 362415 的数字从小到大顺序将对应的密文字符排列，即可得到明文。

2.2.4　一次一密钥密码

顾名思义，一次一密钥密码就是指每次都使用一个新的密钥进行加密，然后该密钥就被丢弃，下次加密时再选择一个新密钥。一次一密钥密码是一种理想的加密方案。一次一密钥密码的密钥就像每页都印有密钥的簿子一样，称为一次一密密钥本（One—TimePad）。一次一密密钥本就是一个包括多个随机密钥的密钥字母集，其中每一页上记录一条密钥。

使用一次一密密钥本加密的过程类似于日历的使用过程，每使用一个密钥加密一条信息后，就将该页撕掉作废，下次加密时再使用下一页的密钥。

发送者使用密钥本中每个密钥字母串加密一条明文字母串的过程，就是将明文字母串和密钥本中的密钥字母串进行模 26 加法运算。

接收者有一个同样的密钥本，并依次使用密钥本上的每个密钥去解密密文的每个字母串。在解密信息后，同样销毁密钥本中用过的一页密钥。

例如，如果信息是：

ONETIMEPAD

密钥本中的一页密钥是：

GINTBDEYWX

则可得到密文：

VWSNKQJOXB

这是因为：

(O+G) mod 26=V

(N+I) mod 26=W

(E+N) mod 26=S

……

这样，加密后得到的密文与明文的位数相同。

如果破译者不能得到加密信息的密钥本，那么该方案就是安全的。由于每个密钥序列都是等概率的（因为密钥是以随机方式产生的），破译者没有任何信息对密文进行密码分析。

如果接收者选择的密钥是：

QIPVLAPFIN

则解密后可得明文为：

ENCRYPTION

如果接收者选择的密钥是：

RRPVLAPFIN

则解密后可得明文为：

DECRYPTION

可见，选择不同的密钥就能得到不同的明文。由于密钥是等概率的，得到的明文也是等概率的，因此绝大多数明文是不可理解的。即使是像上述两例的明文一样碰巧是有意义的，解密者也没有办法确定哪个明文是正确的。随机密钥序列异或随机的明文信息，产生完全随机的密文信息，再大的计算能力对它也无能为力。

一次一密钥的密钥字母必须是随机产生的。对这种方案的攻击实际上是依赖于产生密钥序列的方法。不要使用伪随机序列发生器产生密钥，因为它们通常有非随机性。如果采用真随机序列发生器产生密钥，这种方案就是安全的。

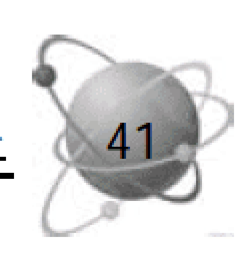
一次一密钥密码在今天仍有应用场合，主要用于高度机密的低带宽信道。

2.3 对称密钥密码体制

2.3.1 对称密钥密码的概念

1. 对称密钥密码体制的基本思想

对称密钥密码体制也叫传统密钥密码体制，其基本思想就是“加密密钥和解密密钥相同或相近”，由其中一个可推导出另一个。使用时两个密钥均须保密，因此该体制也叫单密钥密码体制或私有密钥密码体制。对称密钥密码体制模型如图 2-3 所示。



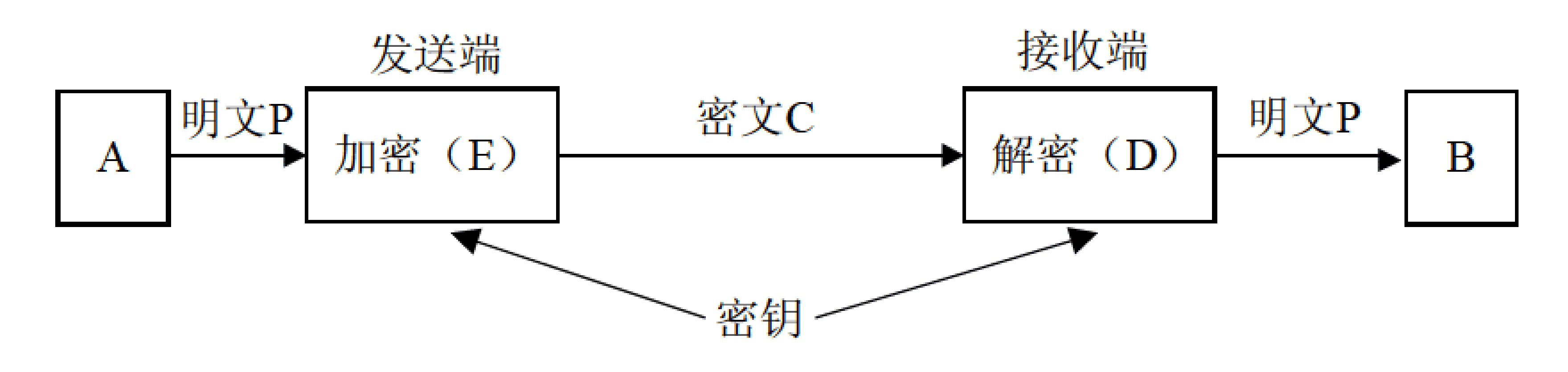


图 2-3　对称密钥密码体制模型

2．对称密钥密码体制的工作流程

对称密钥密码体制的工作流程是：假定 A 和 B 是两个系统，二者决定进行保密通信；A 和 B 通过某种方式获得一个可共用的密钥，该密钥只有 A 和 B 知道，其他用户都不知道；A 或 B 通过使用该密钥加密发送给对方的信息，只有对方可以解密该信息，其他用户均无法解密该信息，这样就达到了信息传输的保密性目的。

2.3.2　数据加密标准 DES

由 IBM 公司开发的数据加密标准（Data Encryption Standard，DES）算法，于 1977 年被美国政府定为非机密数据的数据加密标准。DES 算法是第一个向公众公开的加密算法，也是迄今为止应用得最广泛的一种商用数据加密方案。

DES 算法是最具代表性的分组加密算法。它将明文按 64bit 分组，输入的每一组明文在密钥控制下，也生成 64bit 的密文。密钥的长度为 64bit，其中有 8bit 奇偶校验，因此密钥的有效长度为 56bit。DES 的整个体制是公开的，系统的安全性完全依赖于密钥的保密性。

DES 算法的构成框图如图 2-4 所示。

64bit的明文
↓
初始置换 IP
↓
乘积变换（在密钥控制下的 16 次迭代）
↓
逆初始变换 IP^{-1}
↓
64bit的密文

图 2-4　DES 算法框图

1．初始置换 IP

对输入的 64bit 明文按初始置换表（见图 2-5）进行初始置换。该表描述了置换后的明文信息流中各 bit 的新位置。例如，输入的明文中的第 58bit 信息被置换到了第 1bit 的位置，输入的明文中的第 50bit 信息被置换到了第 2bit 的位置，依此类推。

从图 2-5 中可以看出，IP 中各列元素标明的位置数均相差 8，相当于将原明文各字节按列写出，各列 bit 经过偶采样和奇采样置换后，再对各行进行逆序。

2．乘积变换

乘积变换是 DES 算法的核心部分。经过初始置换后的 64bit 输出作为乘积变换的输入 X_0，其左、右各 32bit 分别记为 L_0 和 R_0，然后经过 16 次迭代。每次迭代时只对上次迭代结果 $X_{i-1}(i=1, \ldots, 16)$ 的右半部分（32bit）R_{i-1} 进行一系列的加密变换。在每次迭代即将结

束时，将上次迭代结果 X_{i-1} 的左半部分（32bit）L_{i-1} 与经过加密变换的 R_{i-1} 逐位模 2 相加，作为本次迭代结果 X_i 的右半部分 R_i，并将 R_{i-1} 作为本次迭代结果 X_i 的左半部分 L_i。最后一次迭代之后，不作左右交换，这是为了使算法既能加密也能解密。每一次迭代时，R_i 都要依次经过扩展置换 E、密钥加密、压缩运算 S、置换运算 P。下面简单介绍这些步骤。

（1）扩展置换 E

扩展置换 E 将输入的 32bit R_{i-1} 扩展为 48bit 的输出。这是通过对部分 bit（原位置数对 4 取模余数为 0 或 1 的 bit）重复使用来完成的。

图 2-6 给出了扩展置换表 E，将表中数据逐行读出即可得到 48bit 的输出。

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

图 2-5　初始置换表 IP

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

图 2-6　扩展置换表 E

（2）密钥加密

密钥加密运算将子密钥产生器输出的 48bit 子密钥 K_i 与扩展置换 E 输出的 48bit 数据按 bit 模 2 相加。

子密钥的生成过程如图 2-7 所示。

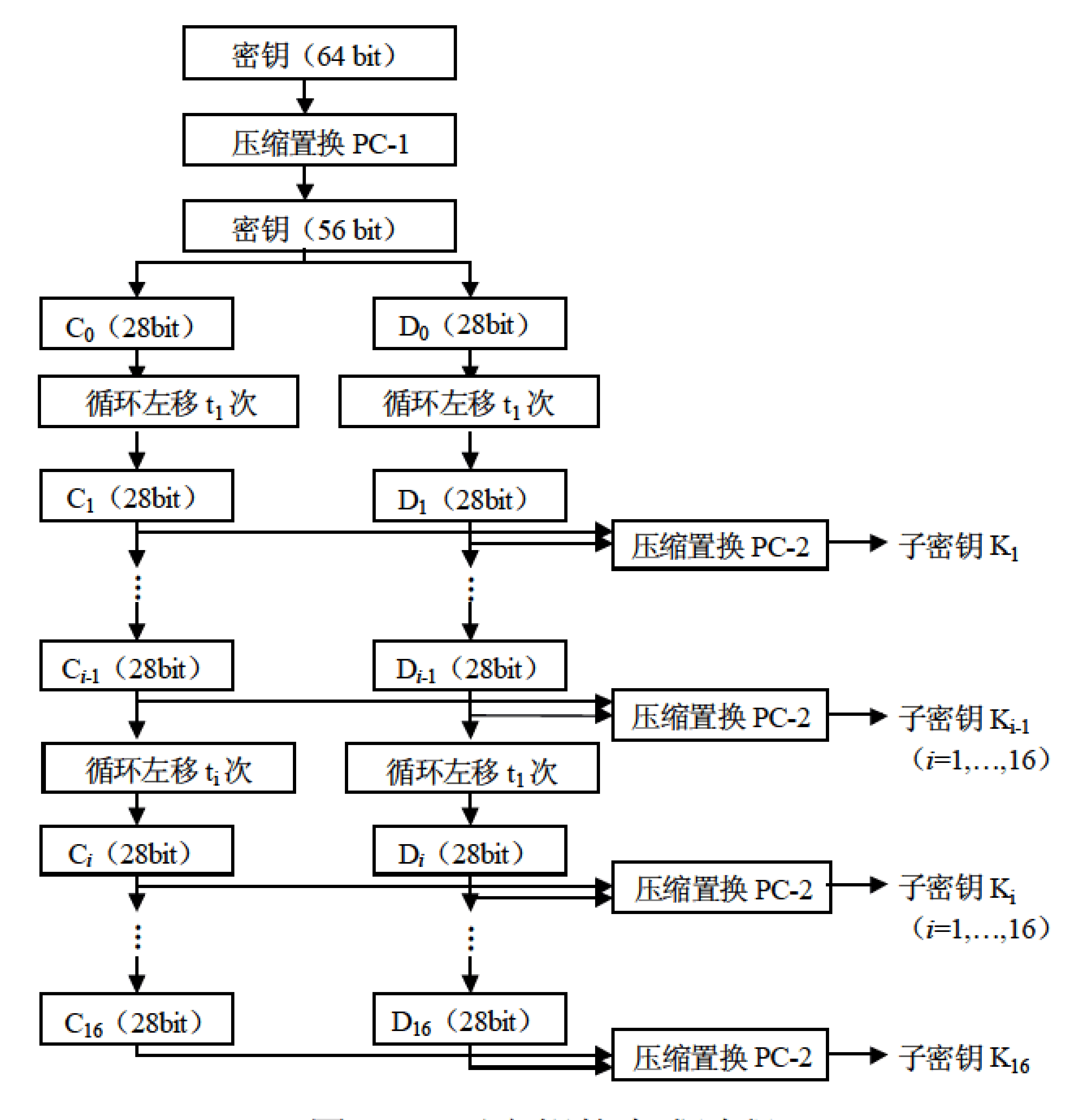


图 2-7　子密钥的生成过程

64bit 初始密钥中有效的 56bit 用于子密钥计算。首先按照密钥压缩置换表 PC-1（见图 2-8）进行压缩置换，得到不含校验信息的 56bit 输出。将这 56bit 分成左、右两组（各 28bit），分别记为 C_0 和 D_0。C_0 和 D_0 各自作循环左移，先后生成 C_1 和 D_1……直至 C_{16} 和 D_{16}。每次迭代中，循环左移的次数如图 2-9 所示。最后，对于每个 C_i 和 D_i 组成的 56bit，按照压缩置换表 PC-2（见图 2-10）进行压缩置换，形成了 48bit 的子密钥 K_i。

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

图 2-8　密钥压缩置换表 PC-1

第 i 次迭代	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
循环左移次数 t_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

图 2-9　循环左移次数表

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

图 2-10　密钥压缩置换表 PC-2

（3）压缩运算 S

压缩运算 S 将经加密运算后得到的 48bit 数据从左到右分成 6bit 一组，8 组数据分别输入 8 个 S 盒中，每个 S 盒实现输入 6bit 到输出 4bit 的替代。图 2-11 给出了 S 盒（S_1～S_8）的替代关系表。

对于每一组输入（6bit），第 1bit 和第 6bit 合起来决定选择 S 盒替代关系表的哪一行，第 2～5bit 共同决定选择 S 盒替代关系表的哪一列，这样就可以确定输出的 4bit 是什么。例如，向 S_1 中输入一个二进制数 110010 时，第 1bit（1）和第 6bit（0）合起来为 10，由此选择替代关系表中 S_1 的第 2 行，由第 2～5bit（1001）决定选择替代关系表中 S_1 的第 9 列，查表知，第 2 行第 9 列的值为 12，从而输出 1100。

（4）置换运算 P

置换运算 P 对 S 盒输出的数据按照置换运算表 P（见图 2-12）进行置换。

行＼列		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1盒	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2盒	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3盒	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4盒	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5盒	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6盒	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7盒	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8盒	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	12
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

图 2-11　S 盒（S_1～S_8）的替代关系表

16	7	20	21
29	12	28	17
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

图 2-12　置换运算表 P

3．逆初始置换 IP^{-1}

将 16 次迭代后输出的 $L_{16}R_{16}$（64bit）按照逆初始置换表 IP^{-1}（见图 2-13）进行置换，得到所需的密文。

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

图 2-13　逆初始置换表 IP^{-1}

4．解密

由密文到明文的解密处理和由明文到密文的加密处理类似。两者使用同一组子密钥，不同的只是两者的生成次序正好相反，即解密时用到的第一个子密钥 K_1 是加密时最后生成的子密钥 K_{16}，依此类推。

下面对比一下使用 DES 算法进行加密和解密的处理过程。

（1）加密过程

L_0R_0←64bit 明文经 IP 置换

L_i←R_{i-1} (i=1,…,16)

R_i←L_{i-1}　　f(K_i,R_{i-1})（i=1,…,16）

64bit 密文 bit←$R_{16}L_{16}$ 经 IP^{-1} 置换

（2）解密过程

$R_{16}L_{16}$←64bit 密文经 IP 置换

R_{i-1}←L_i (i=16,…,1)

L_{i-1}←R_i　　f(K_i, L_I)（i=1,…,16）

64bit 密文 bit←R_0L_0 经 IP^{-1} 置换

DES 算法作为第一个公开的密码体制，由于加密函数的复杂性和 16 轮运算，至今还未发现对 DES 算法存在实际可行的密码分析方法，攻击的方法目前还只能是穷举密钥。

不过，DES 算法也引起了广泛的争论，焦点集中在它把 56bit 作为密钥的长度，人们在 256 密钥空间对目前的计算能力是否切实可行的问题上产生了分歧。有人曾设想设计专门的破译计算机遍历搜索，但没有实际的试验报道。随着 Internet 的发展，网中连接的计算机（大多数是 PC 机）多达数百万台（目前数量还在继续增加），其所拥有的巨大计算能力在向 DES 算法的挑战中充分显示了力量。美国科学家从 1997 年 3 月 13 日开始，在 Internet 上数万名志愿者的协同努力下，历经 96 天，成功地破译了 DES 算法密钥，这是 DES 算法问世以来第一次宣布被人攻破。

DES 算法的被攻破在现代密码学史上是一件非常重大的事件，它意味着在坚定的破译者面前，DES 算法已不再安全。实际计算能力不仅在于超级计算机的进步（以现代技术条件，超级计算机的发展是可以想象的），但同时应该更清楚地看到另一种新的计算资源——大型互联网络的分布计算能力是无法估计的，网上分布的几百万台计算机每秒并行计算次数本身就是一个天文数字。DES 密码体制的被破译，实际上并不是 DES 体制本身存在缺陷（DES 算法设计的成功之处就在于，密码分析者要实现破译，只能采用穷举的方法），只能说明 56bit 的密钥长度显然在不断发展的计算机技术面前已是脆弱的。目前的倾向是使用 128bit 密钥。

5．DES 的特点及应用

（1）DES 算法的特点

DES 算法具有算法容易实现、速度快、通用性强等优点；但也有密钥位数少、保密强度较差和密钥管理复杂等缺点。

（2）DES 的主要应用

① 计算机网络通信。对计算机网络通信中的数据提供保护是 DES 的一项重要应用，但这些保护的数据一般只限于民用敏感信息，即不在政府确定的保密范围之内的信息。

② 电子资金传送系统。采用 DES 的方法加密电子资金传送系统中的信息，可准确、快速地传送数据，并可较好地解决信息安全的问题。

③ 保护用户文件。用户可自选密钥，用 DES 算法对重要文件加密，防止未授权用户窃密。

④ 用户识别。DES 还可用于计算机用户识别系统中。

2.3.3 对称密码体制的其他算法简介

除 DES 外，对称密钥密码算法还有 TDEA（3DES）、IDEA、AES、MD5、RC5 等。以下分别介绍 TDEA、IEDA 和 AES 算法。

1. TDEA 算法

针对 DES 算法密钥短的问题，科学家提出在 DES 的基础上采用三重和双密钥加密的方法，这就是三重 DES 算法（Triple Data Encryption Algorithm，TDEA）。

TDEA 算法使用 3 个密钥，执行 3 次 DES 算法，如图 2-14 所示。

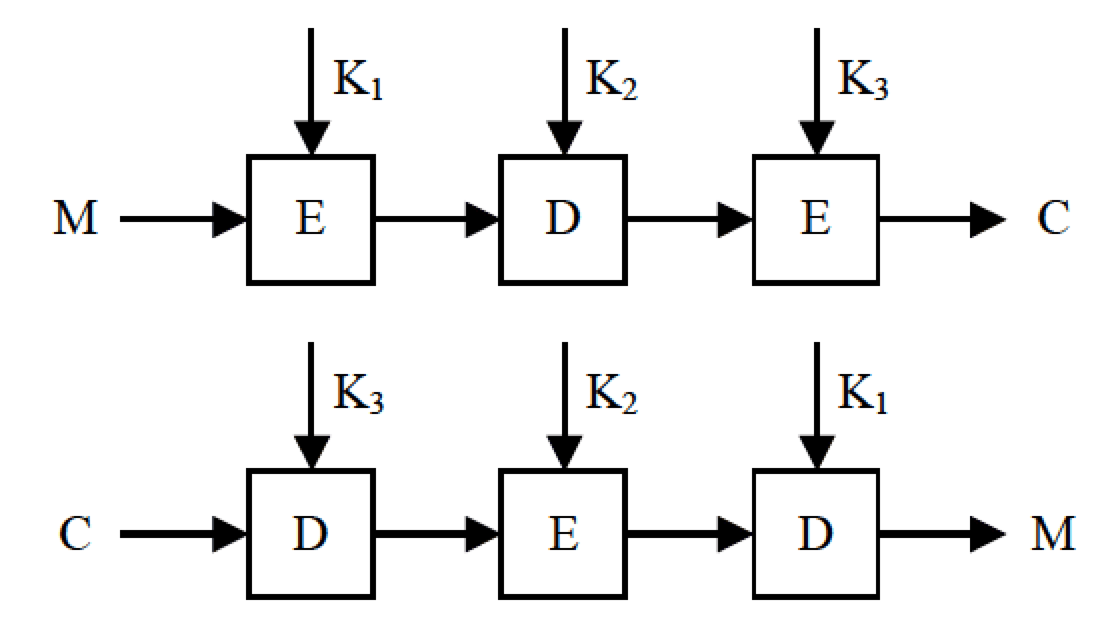


图 2-14　三重 DES 的加密解密过程

加密过程为：

$$C=E_{K3}(D_{K2}(E_{K1}(M)))$$

解密时按密钥相反的顺序进行，可表述为：

$$M=D_{K1}(E_{K2}(D_{K3}(C)))$$

其中 M 表示明文，C 表示密文，$E_K(X)$ 表示使用密钥 K 对 X 进行加密，$D_K(X)$ 表示使用密钥 K 对密文 X 解密。

TDEA 算法使用 2 个 DES 密钥 K_1 和 K_2 进行 3 次 DES 的加密，其效果相当于将密钥长度增加 1 倍。TDEA 算法的执行步骤为：

（1）发送方使用密钥 K_1 进行第一次 DES 加密。

（2）发送方用密钥 K_2 对上一结果进行 DES 解密。

（3）发送方再用密钥 K_1 对上一结果进行第二次 DES 加密。

（4）接收方则相应地使用 K_1 解密，K_2 加密，再使用 K_1 解密。

2. IDEA 算法

国际数据加密算法（International Data Encryption Algorithm，IDEA）是由瑞士的著名学者首先提出的，1990 年被正式公布并在随后得到了增强。这种算法是在 DES 算法的基础上发展起来的，类似于三重 DES。发展 IDEA 也是因为 DES 算法存在密钥太短、容易被攻

破等缺点。

类似于 DES，IDEA 也是一种分组密码算法，分组长度为 64bit，但密钥长度为 128bit。该算法是用 128bit 密钥对 64bit 二进制码组成的数据组进行加密的，也可用同样的密钥对 64bit 密文进行解密变换。

IDEA 与 DES 的明显区别在于循环函数和子密钥生成方法不同。对循环函数来说，IDEA 不使用 S 盒变换，而是依赖于 3 种不同的数学运算——XOR、16bit 整数的二进制加法、16bit 整数的二进制乘法。这些函数结合起来可以产生复杂的转换，且这些转换很难进行密码分析。子密钥生成算法完全依赖于循环移位的应用，但使用方法复杂。

IDEA 算法设计了一系列加密轮次，每轮加密都使用从完整的加密密钥中生成的一个子密钥。每轮次中也使用压缩函数进行变换，只是不使用移位变换。IDEA 中使用异或、模 2^{16} 法和模 $2^{16}+1$ 乘法运算，这 3 种运算彼此混合可产生很好的效果。运算时 IDEA 把数据分为 4 个子分组，每个分组 16bit。

与 DES 的不同之处在于，IDEA 采用软件实现和采用硬件实现同样快速。IDEA 的密钥比 DES 的多一倍，增加了破译难度，被认为是多年后都有效的算法。

由于 IDEA 是在美国之外提出并发展起来的，避开了美国法律上对加密技术的诸多限制，因此有关 IDEA 算法和实现技术的书籍都可以自由出版和交流，可极大地促进 IDEA 的发展和完善。

3. AES 算法

高级加密标准（Advanced Encryption Standard，AES）是由美国国家标准技术研究所（NIST）于 1997 年发起征集的数据加密标准，旨在得到一个非保密的、全球免费使用的分组加密算法，并成为替代 DES 的数据加密标准。NIST 于 2000 年选择了比利时两位科学家提出的 Rijndael 作为 AES 的算法。

Rijndael 是一种分组长度和密钥长度都可变的分组密码算法，其分组长度和密钥长度都分别可为 128bit、192bit 和 256bit。

Rijndael 算法具有安全、高效和灵活等优点，使它成为 AES 最合适的选择。

（1）安全性

Rijndael 算法的频数具有良好的随机特性，其密文比特服从 0.5 的二项式分布，因此其安全性大大增强。它对抗线性攻击和差分攻击的能力也很强。

（2）高效性

由于 Rijndael 算法的线性和非线性混合层都采用矩阵运算，并且其变化轮数（8～12 轮）较少，使得它具有很高的速度。

（3）灵活性

Rijndael 满足了 AES 的要求，密钥长度可为 128bit、192bit 和 256bit，所以可根据不同的加密级别选择不同的密钥长度；其分组长度也是可变的，这正好弥补了 DES 的不足；其循环次数允许在一定范围内根据安全要求进行选取。这些都体现了该算法的灵活性。

2.4 公开密钥密码体制

对称密钥密码体制在加密、解密时使用同样的密钥，这些密钥由发送者和接收者分别保存。该密码体制的主要问题是密钥的生成、管理、分发等都很复杂，特别是随着用户的增加，密钥的需求量成倍增加。如果网络中有 n 个用户，其中每两个用户之间都需要建立保密通信时，则系统中所需的密钥总数达 $n(n-1)/2$ 个，如果两个用户之间可能有多次通信，而每次通信的密钥又不能一样，这样网络中需要的密钥数又将大量增加。在网络通信中，大量密钥的分配是一个很复杂的问题。

2.4.1 公开密钥密码的概念

1. 公钥体制的概念

美国斯坦福大学的两名学者 W. Diffie 和 M. Hellman 于 1976 年在 IEEE Trans. On Information 杂志上发表的文章《New Direction in Cryptography》中，首次提出了“公开密钥密码体制”的概念，开创了密码学研究的新方向。公开密钥密码体制的产生主要有两个方面的原因：一是对称密钥密码体制的密钥分配问题，二是对数字签名的需求。

与对称密钥加密方法不同，公开密钥密码系统采用两个不同的密钥来对信息进行加密和解密，也称为“非对称式加密方法”。由于加密密钥与解密密钥不同，且由其中一个不容易得到另一个，且往往其中一个密钥是公开的，另一个是保密的，因此我们将这种密码体制称为公开密钥密码体制。通常，在这种密码系统中，加密密钥是公开的，解密密钥是保密的，加密和解密算法都是公开的。每个用户有一个对外公开的加密密钥 K_e（称为公钥）和对外保密的解密密钥 K_d（称为私钥）。

虽然理论上解密密钥可由加密密钥推算出来，但这种算法设计在实际中是不可能的；或者虽然能够由加密密钥推算出解密密钥，但要花费很长的时间，因而成为不可行的；所以，将加密密钥公开也不会危害密钥的安全。公开密钥加密算法和解密算法都是公开的。虽然保密密钥是由公开密钥决定的，但却不能由公开密钥计算出来。

自公钥加密体制问世以来，学者们提出了多种公钥加密方法，如 RSA、背包算法、Elgamal、Rabin、DH 等，其安全性都是基于复杂的数学难题。根据所基于的数学难题来区分，有以下 3 类系统算法目前被认为是安全有效的：大整数素因子分解系统（代表性的算法是 RSA）、椭圆曲线离散对数系统（ECC）和离散对数系统（代表性的算法是 DSA）。

（1）当前最著名、应用最广泛的公钥系统的密码算法是 RSA，它的安全性是基于大整数素因子分解的困难性，而大整数因式分解问题是数学上的著名难题，至今没有有效的方法可以解决，因此可以确保 RSA 算法的安全性。

（2）椭圆曲线加密算法（Elliptic Curve Cryptography，ECC）是基于离散对数的计算困难性。它与 RSA 方法相比，具有安全性能更高、运算量小、处理速度快、存储空间占用

小、带宽要求低等优点。因此，ECC 系统是一种安全性更高、算法实现性能更好的公钥系统。

（3）数字签名算法（Data Signature Algorithm，DSA）是基于离散对数问题的数字签名标准，它仅提供数字签名功能，不提供数据加密功能。

2. 公钥体制的特征

（1）用 K_e 对明文加密后，再用 K_d 解密，即可恢复出明文，即：

$$M=D_{k_d}\{E_{k_e}(M)\}$$

（2）加密和解密运算可以对调，即：

$$M=D_{k_d}\{E_{k_e}(M)\}=E_{k_e}\{D_{k_e}(M)\}$$

（3）加密密钥不能用来解密，即：

$$M\neq D_{k_e}\{E_{k_d}(M)\}$$

（4）在计算上很容易产生密钥对 K_e 和 K_d，但已知 K_e 是不能推导出 K_d 的，或者说从 K_e 得到 K_d 是“计算上不可能的”。

3. 公钥算法的应用

使用公开密钥对文件进行加密传输的实际过程包括如下 4 个步骤：

（1）发送方生成一个加密数据的会话密钥，并用接收方的公开密钥对会话密钥进行加密，然后通过网络传输到接收方。

（2）发送方对需要传输的文件用会话密钥进行加密，然后通过网络把加密后的文件传输到接收方。

（3）接收方用自己的私钥对发送方加过密的会话密钥进行解密后得到加密文件的会话密钥。

（4）接受方用会话密钥对发送方加过密的文件进行解密得到文件的明文形式。

因为只有接收方才拥有自己的私钥，所以即使其他人得到了经过加密的会话密钥，也因为没有接收方的私钥而无法进行解密，也就保证了传输文件的安全性。实际上，上述文件传输过程中实现了两个加密、解密过程——文件本身的加密和解密与私钥的加密和解密，这分别通过对称密钥密码体制的会话密钥和公开密钥密码体制的私钥和公钥来实现。

2.4.2 RSA 算法

1. RSA 算法简介

目前，最著名的公开密钥密码算法是 RSA，它是由美国麻省理工学院 MIT 的 3 位科学家 Rivest、Shamir 和 Adleman 于 1976 年提出的，故名 RSA，并在 1978 年正式发表。RSA 是公钥系统最具有典型意义的算法，其优点主要是原理简单、易于使用，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

在此不介绍 RSA 的理论基础（复杂的数学分析和理论推导），只简单介绍其密钥的选取和加密、解密的实现过程。

假设用户 A 在系统中要进行数据加密和解密，则可根据以下步骤选择密钥和进行密码

变换。

（1）随机地选取两个不同的大素数 p 和 q（一般为 100 位以上的十进制数）予以保密。

（2）计算 $n=p\cdot q$，作为 A 的公开模数。

（3）计算 Euler 函数：

$$\Phi(n)=(p-1)\cdot(q-1) \bmod n$$

（4）随机地选取一个与 $(p-1)\cdot(q-1)$ 互素的整数 e，且 $e<\Phi(n)$，作为 A 的公开密钥。

（5）用欧几里德算法，计算满足同余方程

$$e\cdot d\equiv 1\ (\mathrm{mod}\Phi(n))$$

的解 d，作为 A 用户的保密密钥。

（6）任何向 A 发送明文的用户，均可用 A 的公开密钥 e 和公开模数 n，根据式

$$C=M^e\ (\mathrm{mod}\ n)$$

计算出密文 C。

（7）用户 A 收到 C 后，可利用自己的保密密钥 d，根据式

$$M=C^d\ (\mathrm{mod}\ n)$$

还原出明文 M。

2. RSA 算法举例

现以 RSA 算法为例，对明文 HI 进行加密。

（1）选择密钥

设 $p=5$，$q=11$，则：

$$n=55，\Phi(n)=40$$

取 $e=3$（公钥），根据 $e\cdot d\equiv 1\ (\mathrm{mod}\Phi(n))$，则可得：

$$d=27\text{（私钥）}$$

（2）加密

设明文编码为：空格=00，A=01，B=02,…,Z=26，则明文 HI=0809

$$C_1=(08)^3 \bmod 55=17$$

$$C_2=(09)^3 \bmod 55=14$$

Q=17，N=14

所以，HI 的密文为 QN。

（3）恢复明文

$$M_1=C^d\ \mathrm{mod}n=(17)^{27} \bmod 55=08$$

$$M_2=C^d\ \mathrm{mod}n=(14)^{27} \bmod 55=09$$

因此，明文为 HI。

3. RSA 算法的特点及应用

RSA 算法具有密钥管理简单（网上每个用户仅需保密一个密钥，且不需配送密钥）、便于数字签名、可靠性较高（取决于分解大素数的难易程度）等优点，但也具有算法复杂、加密/解密速度慢、难于用硬件实现等缺点。因此，公钥密码体制通常被用来加密关键性的、

核心的、少量的机密信息，而对于大量要加密的数据通常采用对称密钥密码体制。

RSA 算法的安全性建立在难于对大整数提取因子的基础上，已知的证据都表明大整数因式分解问题是一个极其困难的问题，但是随着分解大整数方法的进步及完善、计算机速度的提高以及计算机网络的发展，要求作为 RSA 加密/解密安全保障的大整数越来越大。

RSA 算法的保密性取决于对大素数因式分解的时间。假定用 10^6 次/秒的计算机进行运算，用最快的公式分解 n=100 位十进制数要用 74 年，分解 200 位数要用 3.8×10^9 年。可见，当 n 足够大时（p 和 q 各为 100 位时，n 为 200 位），对其进行分解是很困难的。可以说，RSA 的保密强度等价于分解 n 的难易程度。

RSA 算法为公用网络上信息的加密和鉴别提供了一种基本的方法。它通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。

2.4.3　混合加密方法

以 DES 为代表的对称密钥密码算法的特点是：算法简单，加/解密运算速度快；但其密钥管理复杂，不便于数字签名。

对称密钥密码系统的安全性依赖于以下两个因素：第一，加密算法必须足够强，仅仅基于密文本身去解密信息在实践上是不可能的；第二，加密系统的安全性依赖于密钥的保密性，而不是算法的保密性。对称密钥密码系统的算法实现速度很快，软件实现的速度都可达到每秒数兆或数十兆比特。还是基于这些特点，对称密钥密码系统得到了广泛的应用。因为该算法不需要保密，所以制造商可以大规模开发、生产低成本的芯片以实现数据加密。对称密钥密码系统最大的问题是密钥的分发和管理非常复杂、代价高昂，尤其对于大型网络，密钥的分配和保存就成了大问题；其另一个缺点是不便于实现数字签名。

公开密钥密码系统的优点是密钥管理方便（具有 n 个用户的网络仅需要 $2n$ 个密钥）和便于实现数字签名。因此，最适合于电子商务等应用需要。但是，因为公开密钥密码系统是基于尖端的数学难题，计算非常复杂，但它的加密/解密速度却远赶不上对称密钥加密系统。因此，在实际应用中，公开密钥密码系统并没有完全取代对称密钥密码系统，而是采用相互结合（混合）的方式，如图 2-15 所示。

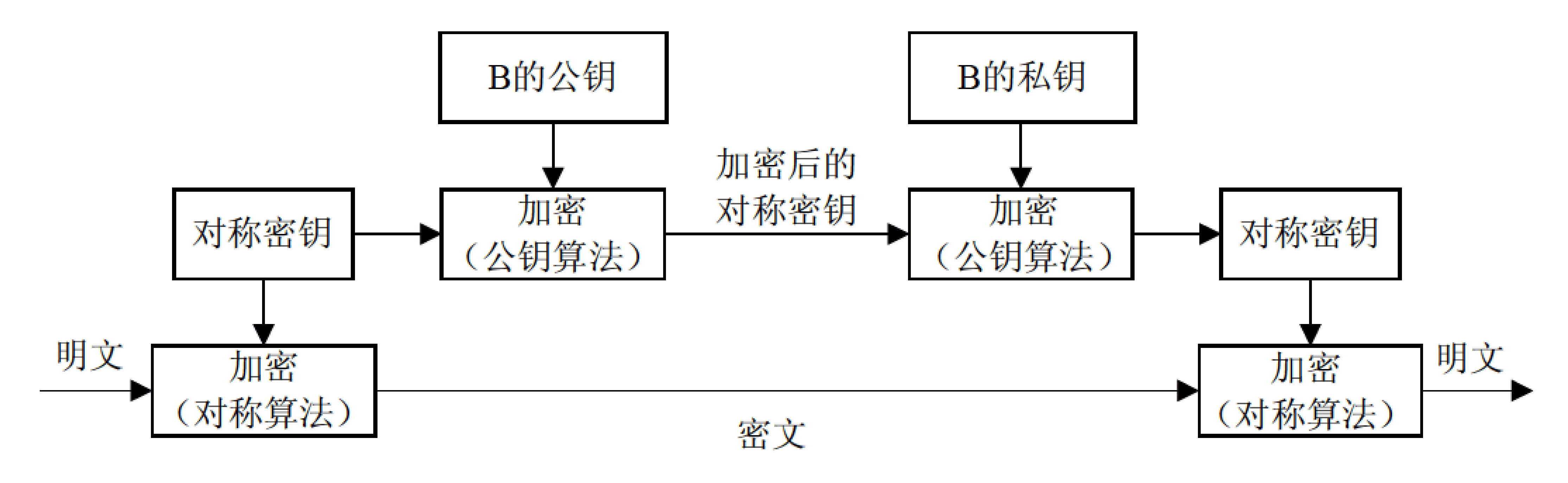


图 2-15　两种密码体制的混合应用

这种混合加密方式可以较好地解决加密/解密运算的速度问题和密钥分配管理问题。其原理是：在发送端，先使用 DES 或 IDEA 对称密钥算法加密数据，然后使用公开密钥算法 RSA 加密前者的对称密钥；到接收端，先使用 RSA 算法解密出对称密钥，再用对称密钥解密被加密的数据。要加密的数据量通常很大，但因对称密钥算法对每个分组的处理仅需很短的时间，因此对大量数据的加密/解密不会影响效率（若使用 DES 加密芯片，则速度会更快）；用 RSA 算法将对称密钥加密后就可公开了，而 RSA 的加密密钥也可以公开，整个系统需保密的只有少量 RSA 算法的解密密钥，因此这些密钥在网络中就很容易被分配和传输了；又因为对称密钥的数据量很少（64/128bit），RSA 只需对其进行 1～2 个分组的加密/解密即可，也不会影响系统的效率。因此，使用这种混合加密方式既可以体现对称密钥算法速度快的优势，也可发挥公钥密钥算法管理方便的优势，二者各取其优，扬长避短。

2.5 数字签名

2.5.1 数字签名概述

在文件上手写签名长期以来被用作签名者身份的证明，或表示同意文件的内容。签名为什么会如此引人注目呢？

（1）签名是可信的。签名使文件的接收者相信签名者是慎重地在文件上签字的。

（2）签名不可伪造。签名证明是签字者而不是其他人在文件上签字。

（3）签名不可重用。签名是文件的一部分，不法之徒不可能将签名移到不同的文件上。

（4）签名的文件是不可改变的。在文件签名后，文件不能改变。

（5）签名是不可抵赖的。签名和文件是物理的东西，签名者事后不能声称他没有签过名。

在现实生活中，关于签名的这些陈述没有一个是完全真实的，如签名能够被伪造，签名能够从文章中盗用移到另一篇文章中，文件在签名后能够被改变……然而，我们之所以愿意与这些问题纠缠在一起，是因为欺骗是困难的，并且还要冒被发现的危险。

我们可以在计算机上实现数字签名，但还存在一些问题。首先，计算机文件易于复制，即使某人的签名难以伪造（例如，手写签名的图形），但是从一个文件到另一个文件复制和粘贴有效的签名都是很容易的，这种签名并没有什么意义；其次，文件在签名后也易于修改，并且不会留下任何修改的痕迹。

公钥密码学使得数字签名成为可能。用私钥加密信息，这时就称为对信息进行数字签名。将密文附在原文后，称为数字签名。其他人用相应的公钥去解密密文，将解出的明文与原文相比较，如果相同则验证成功，这称为验证签名。

现在，已有很多国家制定了电子签名法。《中华人民共和国电子签名法》已于 2004 年 8 月 28 日第十届全国人民代表大会常务委员会第十一次会议通过，并已于 2005 年 4 月 1

日开始施行。

2.5.2　数字签名的方法

基本的数字签名协议是简单的：

（1）Alice 用她的私钥对文件加密，从而对文件签名。

（2）Alice 将签名的文件传给 Bob。

（3）Bob 用 Alice 的公钥解密文件，从而验证签名。

这个协议不需要第三方去签名和验证，甚至协议的双方也不需要第三方来解决争端。如果 Bob 不能完成第三步，那么他知道签名是无效的。

这个协议也满足我们期待的特征：

（1）签名是可信的。当 Bob 用 Alice 的公钥验证信息时，他知道是由 Alice 签名的。

（2）签名是不可伪造的。只有 Alice 知道她的私钥。

（3）签名是不可重用的。签名是文件的函数，并且不可能转换成另外的文件。

（4）被签名的文件是不可改变的。如果文件有任何改变，文件就不可能用 Alice 的公钥验证成功。

（5）签名是不可抵赖的。Bob 不用 Alice 的帮助就能验证 Alice 的签名。

在实际的实现过程中，采用公钥密码算法对长文件签名效率太低。为了节约时间，数字签名协议经常和单向散列函数一起使用。Alice 并不对整个文件签名，只对文件的散列值签名。在这个协议中，单向散列函数和数字签名算法是事先就协商好了的。

（1）Alice 产生文件的散列值。

（2）Alice 用她的私钥对散列值加密，借此表示对文件签名。

（3）Alice 将文件和散列签名送给 Bob。

（4）Bob 用 Alice 发送的文件产生文件的散列值，然后用 Alice 的公钥对签名的散列值解密。如果解密的散列值与自己产生的散列值相同，签名就是有效的。

这样计算速度大大地提高了，并且两个不同的文件有相同的 160bit 散列值的概率极小（$1/2^{160}$）。因此，使用单向散列函数的签名和文件签名一样安全。如果使用非单向散列函数，则可能导致多个不同文件的散列值相同，这样对某一特定的文件签名就可复制为对大量文件的签名。

这个协议还有其他好处。首先，签名和文件可以分开保存。其次，接收者对文件和签名的存储量要求大大降低了。档案系统可用这类协议来验证文件的存在而不需保存它们的内容。中央数据库只存储各个文件的散列值，根本不需要查看文件。用户将文件的散列值传给数据库，然后数据库对提交的文件散列值加上时间标记并保存。如果以后有人对某文件的存在发生争执，数据库可通过查找文件的散列值来解决争端。另外，不对消息本身签名，而对消息的散列值签名可以抵御某些攻击。

实际上，Bob 在某些情况下可以欺骗 Alice，他可能把签名和文件一起重用。如果 Alice 在合同上签名，这种重用不会有什么问题。但如果 Alice 在一张数字支票上签名，这样做

就有问题了。

假若 Alice 交给 Bob 一张签名的数字支票，Bob 把支票拿到银行去验证签名，然后把钱从 Alice 的账户上转到自己的账户上。如果 Bob 心怀不轨，故意保存了数字支票的副本，过了一星期，他又把数字支票拿到银行（也可能是另一家银行），银行验证数字支票后将再次把钱转到他的账户上。只要 Alice 不去核对支票簿清账，Bob 就可以一直干下去。

因此，数字签名经常包括时间标记。对日期和时间的签名附在信息中，并与信息中的其他部分一起签名。银行将时间标记存储在数据库中。现在，当 Bob 第二次想支取 Alice 的支票时，银行就会检查时间标记是否和数据库中的一样。由于银行已经支付了带有这一时间标记的支票，于是报警。

Alice 也有可能用数字签名进行欺骗，并且无人能阻止她。她可能对文件签名，然后声称并没有那样做。首先，她按常规对文件签名，然后以匿名的形式发布她的私钥，或者故意把私钥丢失在公共场所。这样，发现该私钥的任何人都可假冒 Alice 对文件签名，于是 Alice 就声明她的签名受到侵害，其他人正在假冒她签名云云。也就是说，她否认对文件的签名和任何其他的用她的私钥签名的文件，这叫做抵赖。

采用时间标记可以部分地限制这种欺骗，否则 Alice 总可以声称她的密钥在较早的时候就丢失了。如果 Alice 把事情做得很好，她就可以对文件签名，然后成功地声称并没有对文件签名，这应该从法律或制度上来解决。丢失私钥造成的损失应该由私钥拥有者来承担，这就像公章丢失造成的损失应该由该单位来承担一样。

现在讨论一下多重签名。Alice 和 Bob 怎么对同一数字文件签名呢?不用单向散列函数，有两种选择。第一种选择是 Alice 和 Bob 分别对文件的副本签名，结果签名的信息是原文的两倍；第二种就是 Alice 首先签名，然后 Bob 对 Alice 的签名再进行签名，这是可行的，但是在不验证 Bob 的签名的情况下就验证 Alice 的签名是不可能的。

采用单向散列函数，多重签名很容易做到。

（1）Alice 对文件的散列值签名。

（2）Bob 对文件的散列值签名。

（3）Bob 将他的签名交给 Alice。

（4）Alice 把文件、她的签名和 Bob 的签名发给 Carol。

（5）Carol 验证 Alice 和 Bob 的签名。

Alice 和 Bob 能同时或顺序地完成步骤（1）和步骤（2），Carol 可以只验证其中一人的签名而不用验证另一人的签名。

2.5.3 带加密的数字签名

通过把公钥密码和数字签名结合起来，即可产生一个协议，达到将数字签名的真实性和加密的安全性合二为一的目的，如图 2-16 所示。想象你写的一封信：签名提供了原作者的证明，而信封提供了秘密性。

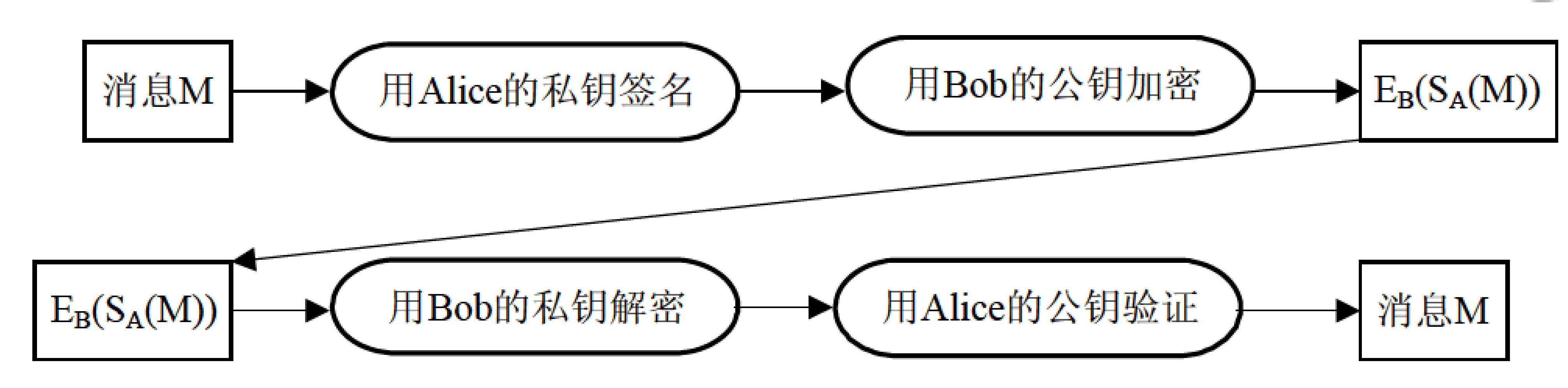


图 2-16　带加密的数字签名

（1）Alice 用她的私钥对信息签名：

$$S_A(M)$$

（2）Alice 用 Bob 的公钥对签名的信息加密，然后发送给 Bob：

$$E_B(S_A(M))$$

（3）Bob 用他的私钥解密：

$$D_B(E_B(S_A(M)))\text{：}\ S_A(M)$$

（4）Bob 用 Alice 的公钥验证并且恢复出信息：

$$V_A(S_A(M))= M$$

加密前签名是很自然的。当 Alice 写一封信时，她在信中签名，然后把信装入信封中。如果她把没签名的信放入信封，然后在信封上签名，那么 Bob 可能会担心是否这封信被替换了。

在电子通信中也是这样，加密前签名是一种谨慎的习惯做法。这样做不仅更安全（其他人不可能从加密信息中把签名移走，然后加上他自己的签名），而且还有法律上的考虑——如果签名者不能见到被签名的文本，那么签名就不具法律效力。

Alice 没有理由必须把同一个公钥/私钥密钥对用于加密和签名。她可以有两个密钥对：一个用于加密，另一个用于签名。分开使用有它的好处：她能够把她的加密密钥交给警察而不泄露她的签名，一个密钥被托管而不会影响到其他密钥，并且密钥能够有不同的长度，能够在不同的时间终止使用。

当然，这个协议应该用时间标记来阻止信息的重复使用。

2.6　密 钥 管 理

在现代密码学研究中，加密算法和解密算法一般都是公开的。当合理的密码算法确定后，密码系统的保密程度就完全取决于密钥的保密程度。因此，密钥管理在整个保密系统中占有极其重要的地位。若密钥得不到合理的保护和管理，即使算法再复杂，保密系统也是脆弱的。密钥管理的目的就是要保证数据保密系统的安全性。

密钥管理包括密钥的产生、密钥的存储和保护、密钥的更新、密钥的分发、密钥的验证、密钥的使用、密钥的销毁等。这些问题的本质就是要正确地解决密钥从产生到使用全过程的安全性和实用性。

密钥管理最主要的过程是密钥的产生、保护和分发；其次，是网络环境下的密钥管理算法。

2.6.1 密钥的产生

密码算法的安全性依赖于密钥，如果采用一个弱的密钥生成方法，那么整个加密体制就是弱的。因为弱的密钥生成算法很容易被破译，密码分析者在破译了密钥后不需要再去破译算法就可以得到他想要的东西了。因此，密钥的产生是密钥管理中的基本问题。

好的密钥是指那些由自动处理设备生成的随机字符串。如果密钥有 64bit 长，每一个可能的 64bit 密钥必须具有相等的可能性。因此，密钥的生成首先要保证所产生的密钥具有良好的随机性，避免出现简单、明显的密钥或一串容易记忆的字符或数字。现代网络的信息量越来越大，需要的密钥量也大，因此密钥的产生要能自动地、大量地进行。

密钥的产生主要利用噪声源技术，该技术可产生二进制的随机序列或与之对应的随机数。其主要理论基础是混沌理论。使用随机序列发生器可以自动地产生大量随机的密钥。

2.6.2 密钥的保护和分发

1. 密钥的分层保护

密钥的分层保护也叫主密钥保护体制，它是以对称密钥为基础的管理体制。该体制可把密钥分为几层，高一层密钥保护低一层密钥。

一般把密钥分为主密钥、辅助主密钥和会话密钥 3 个层次。每个主密钥对多个辅助主密钥进行加密保护，每个辅助主密钥对多个会话密钥进行加密保护。最后，再用会话密钥对传输的具体信息进行加密保护。

该体制的思想就是把网络中大量使用的会话密钥置于辅助主密钥的保护之下，再由极少量的主密钥保护辅助主密钥。经过这样保护后，在接收端各通信点需经过相应的解密才能得到通信所用的会话密钥，从而使会话密钥更安全。

整个网络的密钥的保护与传输都由计算机控制，实现了密钥管理的自动化。

2. 一种会话密钥的保护体制

在用户 A 与 B 的通信系统中，可采用如下步骤分发和保护会话密钥。

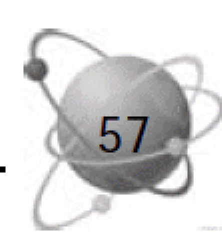
（1）用户 A 产生自己的公钥 K_e 和私钥 K_d。

（2）用户 A 将 K_e 传输给用户 B。

（3）用户 B 用 A 的公钥 K_e 加密自己产生的一个会话密钥 K_s，并传输给 A。

（4）用户 A 用自己的私钥 K_d 解密后得到 K_s。

（5）用户 A 用 K_s 加密要发给 B 的数据；通信结束后，K_s 被清除。



2.6.3　网络环境下的密钥管理算法

Kerberos 是一种使用对称密钥加密算法实现通过可信任的第三方密钥分配中心（Key Distribute Center，KDC）的身份验证系统，其主要功能之一便是解决保密密钥管理与分发的问题。

Kerberos 中有 3 个通信参与方：需要验证身份的通信双方和一个双方都信任的第三方，即 KDC。KDC 可以看作一个秘密密钥源，与 DES 一起使用；也可以是一个公开密钥源。

Kerberos 就是建立在这个安全的、可信赖的密钥分配中心的概念上。建有 KDC 的系统用户只需保管与 KDC 之间使用的密钥加密密钥——与 KDC 通信的密钥即可。

KDC 的工作过程简述如下：

（1）假设用户 A 要与 B 通信，A 先向 KDC 提出申请与 B 的联系和通信会话密钥。

（2）KDC 为用户 A 和 B 选择一个会话密钥 K_s，分别用 A 和 B 知道的密钥进行加密，然后分别传送给 A 和 B。

（3）用户 A 和 B 得到 KDC 加密过的信息后，分别解密，得到会话密钥 K_s。

（4）至此，用户 A 与 B 即可利用 K_s 进行保密通信了。通信结束后，K_s 随即被销毁。

目前，各主要操作系统都支持 Kerberos 验证系统，比如 Windows NT。Kerberos 实际上已成为工业界的事实标准。Kerberos 使用对称密钥算法来实现通过 KDC 的验证服务，它提供了网络通信方相互验证身份的手段，但并不依赖于主机操作系统和地址。

2.7　网络保密通信

2.7.1　通信安全

虽然网络可以使经济、文化、医疗、科学、教育和交通等领域的信息更加有效和迅速地被获取、传输和应用，但如果网络系统和用户缺乏适当的安全保护措施，这些信息很容易在传输过程中被非法获取，以及造成网络系统的其他资源被破坏等，从而使系统遭受重大的损失。为了充分利用网络系统资源，首先就要保证网络系统的通信安全。要保证系统的通信安全，就要充分认识到网络系统的脆弱性，特别是网络通信系统和通信协议的弱点，估计到系统可能遭受的各种威胁，采取相应的安全策略，尽可能地减少系统面临的各种风险，保证计算机网络系统具有高度的可靠性、信息的完整性和保密性。

网络通信系统可能面临各种各样的威胁，例如来自各种自然灾害、恶劣的系统环境、人为破坏和误操作等。所以，要保护网络通信安全，不仅必须要克服各种自然和环境的影响，更重要的是要防止人为因素造成的威胁。

1. 线路安全

通信过程中，通过在通信线路上搭线可以窃取（窃听）传输的信息，还可以使用相应

设施接收线路上辐射的信息，这些都是通信中的线路安全问题。对此应该如何应对呢？

一种简单但很昂贵的电缆加压技术可保护通信电缆安全，该技术是将通信电缆密封在塑料套里深埋于地下，并在线路的两端加压。线路上连接了带有报警器的显示器用来测量压力，如果压力下降，则意味着电缆被破坏，维修人员将被派出去维修出现问题的电缆。另一种电缆加压技术不是将电缆埋于地下，而是架空，每寸电缆都暴露在外。如果有人要割电缆，监视器就会启动报警器，通知安全保卫人员；如果有人在电缆上接了自己的通信设备，安全人员在定期检查电缆时，就会发现电缆的拼接处。加压电缆屏蔽在波纹铝钢包皮中，因此也几乎没有电磁辐射，如果用电磁感应窃密，要使用大量设备，因此很容易被发现。

光缆曾被认为是不可搭线窃听的，因其断裂或破坏处会立即被检测到，拼接处的传输速率是很慢的；光纤没有电磁辐射，所以也不可能有电磁感应窃密。但遗憾的是光纤有长度限制，超过最大长度时要定期地放大信号，就要将信号转变为电脉冲，放大后再恢复为光脉冲继续通过另一条线路传输。完成这一操作的设备（复制器）是光纤通信系统安全的薄弱环节，因为信号极可能在这一环节被窃听。

2. TCP/IP 服务的脆弱性

基于 TCP/IP 协议的服务很多，常用的有 Web 服务、FTP 服务、电子邮件服务等；人们不太熟悉的有 TFTP 服务、NFS 服务、Finger 服务等。这些服务都在不同程度上存在安全缺陷。

（1）电子邮件程序存在漏洞：电子邮件附着的文件中可能带有病毒，邮箱经常被塞满，电子邮件炸弹令人烦恼，还有邮件溢出等。

（2）简单文件传输协议 TFTP 服务用于局域网，它没有任何安全认证，安全性极差，常被人用来窃取密码文件。

（3）匿名 FTP 服务存在一定的安全隐患：有些匿名 FTP 站点为用户提供了一些可写的区域，用户可以上传一些信息到站点上，因此可能会浪费用户的磁盘空间、网络带宽等资源，还可能造成“拒绝服务”攻击。

（4）Finger 服务可查询用户信息，包括网上成员姓名、用户名、最近的登录时间、地点和当前登录的所有用户名等，这也为入侵者提供了必要的信息和方便。

2.7.2 通信加密

网络中的数据加密可分为两个途径，一种是通过硬件实现数据加密，一种是通过软件实现数据加密。通过硬件实现网络数据加密有 3 种方式：链路加密、节点加密和端一端加密；软件数据加密就是指使用前述的加密算法进行加密。

计算机网络中的加密可以在不同层次上进行，最常见的是在应用层、链路层和网络层进行加密。应用层加密需要所使用的应用程序支持，包括客户机和服务器的支持，这是一种高级的加密，在某些具体应用中非常有效，但它不能保护网络链路。数据链路层加密应用于单一网络链路，仅仅在某条链路上保护数据，而当数据通过其他未被保护的链路时则

不被保护；这是一种低级的保护，不能被广泛应用。网络层加密介于应用层加密和数据链路层加密之间，加密在发送端进行，通过不可信的中间网络，到接收端进行解密。

1. 硬件加密和软件加密

（1）硬件加密

所有加密产品都有特定的硬件形式。这些加密/解密硬件被嵌入到通信线路中，然后对所有通过的数据进行加密。虽然软件加密在今天正变得很流行，但硬件加密仍是商业和军事等领域应用的主要选择。选用硬件加密的原因有以下几种。

① 快速

加密算法中含有许多复杂运算，如果用软件实现这些复杂运算，则运算速度将受到很大影响，而特殊的硬件将具有速度优势。另外，加密常常是高强度的计算任务，加密硬件芯片可较好地完成这样的任务并有较快的速度。

② 安全

硬件加密可以使用各种跟踪工具对运行在未加保护的计算机上的加密算法进行跟踪或修改而不被发现；使用硬件加密设备可将加密算法封装保护，以防被修改。例如，针对特殊目的 VISL 芯片，可以覆盖一层化学物质，使得任何企图对其内部进行的访问都将导致芯片逻辑的破坏。

③ 易于安装

大多数加密功能与计算机无关，将专用加密硬件放在电话、传真机或 Modem 中比设置在微处理器中更方便。安装一个加密设备比修改配置计算机系统软件更容易。加密应该是不可见的，它不应该妨碍用户。而软件要做到这样，唯一的办法就是将加密程序写在操作系统软件深处。

（2）软件加密

任何加密算法都可用软件实现。软件实现的不利之处就是速度慢、开销大和易于改动，有利之处是灵活性大和可移植性强，易使用、易升级。

软件加密程序很大众化，并可用于大多数操作系统。这些加密程序可用于保护个人文件，用户通常用手工加密/解密文件。软件加密的密钥管理很重要，密钥不应该存储在磁盘中，密钥和未加密文件在加密后应删除。

2. 通信加密方式

（1）链路加密

链路加密（Link Encryption）是指传输数据仅在数据链路层上进行加密。链路加密是为保护两相邻节点之间链路上传输的数据而设立的。只要把两个密码设备安装在两个节点间的线路上，并装有同样的密钥即可。被加密的链路可以是微波、卫星和有线介质。

在链路上传输的信息（包括信息正文、路由及检验码等控制信息）是密文，而链路间节点上必须是明文。因为在各节点上都要进行路径选择，而路由信息必须是明文，否则就无法进行选择了。这样，信息在中间节点上要先进行解密，以获得路由信息和检验码、进行路由选择和差错检测，然后再被加密，送至下一链路，如图 2-17 所示。

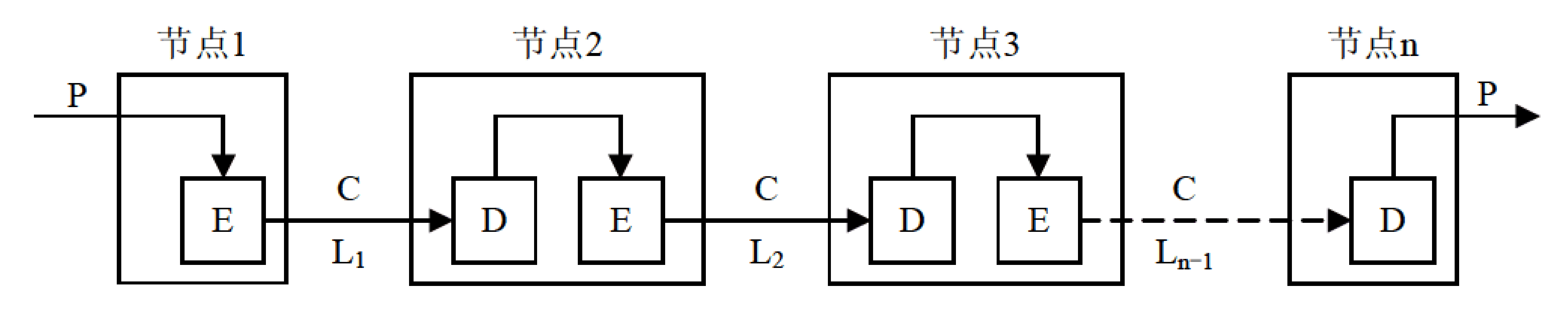


图 2-17 链路加密

使用链路加密装置能为某链路上的所有报文提供保密传输服务，即经过一台节点机的所有网络信息传输均需加、解密，每一个经过的节点都必须有密码装置，以便解密、加密报文。如果报文仅在一部分链路上加密而在另一部分链路上不加密，则相当于都未加密，仍然是不安全的。

数据在到达目的地之前，可能要经过许多通信链路的传输，因此在链路加密中的信息在每台节点机内都要被解密和再加密，依次进行，直至到达目的地。同一节点上的解密和加密密钥是不同的，而同一条链路两端的加密和解密是相关的。

链路加密时由于报头和正文在链路上均被加密，被传输信息的源点与终点得以掩盖，从而可屏蔽掉报文的频率、长度等特征，这样攻击者就得不到这些特征值。因此，链路加密可防止报文流量分析的攻击。

（2）节点加密

为了解决数据在节点中是明文的缺点，出现了一种新的加密方式——节点加密（Node Encryption）。节点加密在中间节点装有加密/解密保护装置，由该装置完成一个密钥向另一个密钥的变换。因而，该方式使得在节点内也不会出现明文。

但节点加密方式与链路加密方式一样，都存在一个共同缺点，即需要公共网络提供商的配合，修改其交换节点，增加安全单元或保密装置。

链路加密仅在通信链路上提供安全性，信息在节点上以明文形式存在，因此所有节点在物理上必须是安全的，否则就会泄漏明文内容。然而保证每一个节点的安全性需要较高的费用。为每一个节点提供加密硬件设备和一个安全的物理环境所需要的费用由以下几部分组成：保护节点物理安全的雇员开销，为确保安全策略和程序的正确执行而进行审计时的费用，以及为防止安全性被破坏时带来损失而参加保险的费用等。

节点加密要求报头和路由信息以明文形式传输，以便中间节点能用来处理信息，因此这种方法对于防止攻击者进行信息流量分析是脆弱的。

（3）端-端加密

端-端加密（End to End Encryption）是传输数据在应用层上完成加密的加密方式。端-端加密可对两个用户之间传输的数据提供连续的安全保护。数据在初始节点上被加密，直到目的节点时才被解密，在中间节点和链路上数据均以密文形式传输。这样信息在整个传输过程中均受到保护，即使有节点被损坏也不会使信息泄露。

端-端加密时，只有在发送端和接收端才有加密和解密设备，中间各节点不需要有密码设备。因此，同链路加密相比，可减少很多密码设备。另一方面，由于信息由报头和报文组成，报文为传输的信息，报头为路由等控制信息，在网络中传输时要涉及到路由选择。

链路加密时，报文和报头两者都被加密，而在端-端加密时，各中间节点虽不进行解密，但必须检查报头信息，所以路径选择等控制信息不能被加密，必须是明文。即端-端加密只能对信息的正文（报文）进行加密，而不能对报头加密，如图 2-18 所示。

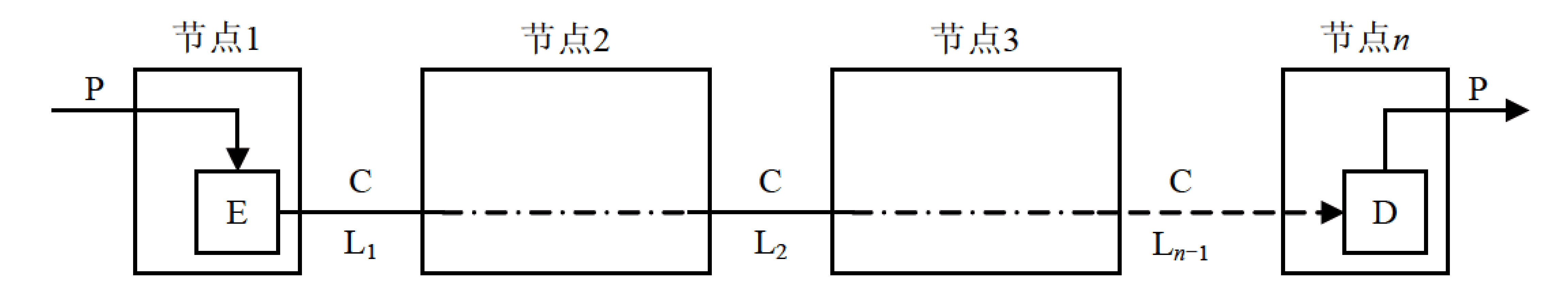


图 2-18　端-端加密

端-端加密系统的价格便宜些，并且与链路加密和节点加密相比更可靠，更容易设计、实现和维护。端-端加密还避免了其他加密系统所固有的同步问题，因为每个报文包均是独立被加密的，所以一个报文包所发生的传输错误不会影响后续的报文包。此外，从用户对安全需求的直觉上讲，端-端加密更自然些。单个用户可能会选用这种加密方法，以便不影响网络上的其他用户。

端-端加密系统通常不允许对信息的目的地址进行加密，这是因为每一个信息所经过的节点都要用此地址来确定如何传输信息。由于这种加密方法不能掩盖被传输信息的源点与终点，因此它对于防止信息流量分析攻击也是脆弱的。

（4）通信加密方式的比较和选择

常用的通信加密方式是链路加密和端-端加密。链路加密是对一条链路的通信采取的保护措施，而端-端加密则是对整个网络的通信系统采取的保护措施。

① 链路加密的特点：加密方式比较简单，实现也较容易；可防止报文流量分析的攻击；一个链路被攻破，不影响其他链路上的信息；一个中间节点被攻破时，通过该节点的所有信息将被泄露；加密和维护费用大，用户费用很难合理分配；链路加密只能认证节点，而不面向用户，因此链路加密不能提供用户鉴别。

② 端-端加密的特点：可提供灵活的保密手段，例如主机到主机、主机到终端、主机到进程的保护；加密费用低，并能准确分配；加密在网络应用层实现，可提高网络加密功能的灵活性；加密可使用软件实现，使用起来很方便；不能防止信息流量分析攻击；整个通信过程中各分支相互关联，任何局部遭到破坏时将影响整个通信过程；端-端加密对用户是可见的，可以看到加密后的结果，起点、终点很明确，可以进行用户认证。

③ 加密方式的选择：从以上两种加密方式可知，链路加密对用户系统比较容易，使用的密钥较少，而端-端加密比较灵活。因此，用户在选择通信方式时可作如下考虑：在需要保护的链路数少，且要求实时通信，不支持端-端加密的远程调用等通信场合，宜采用端-端加密方式；在多个网络互联的环境中，宜采用端-端加密方式；在需要抵御信息系统流量分析场合，可采用链路加密和端-端加密相结合的加密方式。

总而言之，与链路加密方式相比，端-端加密具有成本低、保密性强、灵活性好等优点，因此应用更为广泛。

2.8 加密软件 PGP

目前电子邮件和在网络上输入文件已经成为人们工作、生活中不可缺少的一部分，在我们尽情享受其带来的大便利的同时，安全问题也变得日益突出。如果不注意保护自己的信息，随意地将未经加密的数据在 Internet 上传输，很容易被第三者截获，造成隐私泄露。这便涉及到加密问题。此外，还衍生出相关信息的认证问题，如让收信人确认邮件没有被第三者篡改，就需要使用数字签名技术。在此情形下，PGP 应运而生。

2.8.1 PGP 概述

PGP（Pretty Good Privacy）是一个广泛应用于电子邮件和文件加密的软件，一经推出，备受青睐，已成为电子邮件加密的事实标准。

PGP 把 RSA 公钥体系的密钥管理方便和传统加密体系的高速度结合起来，并且在数字签名和密钥认证管理机制上有着巧妙的设计。虽然 PGP 主要是基于公钥加密体系的，但它不是一种完全的公钥加密体系，而是一种混合加密算法。它是由一个对称加密算法（IDEA）、一个非对称加密算法（RSA）、一个单向散列算法（MD5）以及一个随机数产生器组成的，每种算法都是 PGP 不可分割的组成部分。PGP 之所以得到大家的认可，最主要是它集中了几种加密算法的优点，使它们彼此得到互补。

PGP 的巧妙之处在于它汇集了各种加密方法的精华。PGP 实现了目前大部分流行的加密和认证算法，如 DES、IDEA、RSA 及 MD5、SHA 等算法。

PGP 软件兼有加密和签名两种功能。它不但可以对用户的邮件进行保密，以防止非授权者阅读，还能对邮件进行数字签名，使收信人确信邮件未被第三者篡改过。在 PGP 中，主要使用 IDEA 算法对数据进行加密（因为它速度快，安全性好）；使用 RSA 算法对 IDEA 的密钥进行加密（因为 RSA 公钥算法的密钥管理方便）。这样，两类体制的算法结合在一起实现加密功能，突出了各自的优点。PGP 还使用 MD5 作为散列函数，对数据的完整性进行保护，并与加密算法结合，提供数字签名功能。PGP 的加密功能和签名功能可以单独使用，也可以同时使用。

PGP 还可以只签名而不加密，这适用于用户公开发布信息的情况。用户为了证实自己的身份，在发送信件时往往用自己的私钥签名，这样就可以让收信人确认发信人的身份，也可以防止发信人进行抵赖，这一点在商业领域有很大的应用前途。

PGP 给邮件加密和签名的过程是这样的：首先甲用自己的私钥将由 MD5 算法得到的 128bit 的“邮件摘要”加密（即签名），附加在邮件后；再用乙的公钥将整个邮件加密（注意这里的次序，如果先加密再签名，别人可以将签名去掉后签上自己的名，从而篡改了签名）。乙收到后，用自己的私钥将邮件解密，得到甲的原文和签名；然后利用 MD5 算法从原文计算出一个 128bit 的特征值，再将其与用甲的公钥解密签名所得到的数据进行比较。

如果比较相符，则说明这份邮件确实是甲寄发的。这样，保密性和认证性要求都得到了满足。

2.8.2 PGP 提供的服务

PGP 除提供数据加密和数字签名服务外，还提供数据压缩和转换服务，这些服务都是与信息和文件格式相关的。

1. 数字签名

PGP 提供的数字签名服务包括 Hash 编码或消息摘要的使用、签名算法以及公钥加密算法。它提供了对发送方的身份验证，其步骤如下。

（1）发送方生成所要发送的信息。

（2）发送方产生消息的 Hash 编码。

（3）用发送方的私钥加密 Hash 编码。

（4）将加密后的 Hash 编码附在原始消息上。

（5）接收方使用发送方的公钥对加密的 Hash 编码进行解密。

（6）接收方产生所接收信息的 Hash 编码，并与解密的 Hash 编码进行比较，如果两者相同，则认为信息是可信任的。

一般情况下，签名附着于被签署的信息或文件上，但 PGP 也支持分离的签名。分离签名可以独立于它所签署的信息而被存储和传输，有时这是很有用的。比如用户可能希望为所有发送和接收的信息维护一个单独的签名日志；对于可执行文件而言，分离签名能检测出随后的病毒感染；当多个实体签署诸如合同之类的一个文档时，使用分离签名更有其方便之处。

2. 数据加密

PGP 通过使用对称加密算法 IDEA 对要传送的信息或在本地存储的文件进行加密。在 PGP 中，对于每个要加密的消息，都会产生随机的 128bit 新密钥。由于每个密钥仅使用一次，所以可将会话密钥和消息绑定在一起进行传送。传送时为了保护会话密钥，再使用接收方的公钥将其加密。数据加密服务的步骤如下：

（1）发送方生成所要发送的消息。

（2）发送方产生仅适用于该信息的随机数字作为会话密钥。

（3）发送方使用会话密钥加密信息。

（4）发送方用接收方的公钥加密会话密钥，并附在加密信息上。

（5）接收方使用自己的私钥解密出会话密钥。

（6）接收方使用会话密钥解密出信息。

3. 数据压缩

默认情况下，PGP 在数字签名和加密服务之间提供压缩服务，即 PGP 先对信息进行签

名，然后再进行压缩，最后再对压缩的信息进行加密。

PGP 在加密数据前先对其进行预压缩处理（PGP 内核使用 PKZIP 算法来压缩加密前的明文），好处有两点。一方面对电子邮件而言，加密经过压缩的信息所得到的密文有可能比明文更短，这就节省了网络传输的时间；另一方面，明文经过压缩，实际上相当于经过一次变换，信息更加杂乱无章，对明文攻击的抵御能力更强。PKZIP 算法是一个公认的压缩率和压缩速度都相当好的压缩算法。PGP 中使用 PKZIP 算法是经过原作者同意的。

4. 格式转换

使用 PGP 时，传送的消息块通常是部分加密的。如果只使用数字签名服务，则消息摘要是加密的；如果使用了数据加密服务，则消息和签名都是加密的。这样，部分或全部的结果将由任意的 8 位字节流组成，而很多电子邮件只允许使用纯 ASCII 文本。为了适应这种限制，PGP 提供了将原始的 8 位数据流转换为 ASCII 字符串的服务。

2.8.3 PGP 密钥的分发和保护

1. 公钥的分发

对 PGP 来说，公钥本来就是公开的，不存在防偷盗问题，但公钥在发布中仍然存在安全性问题，其中最大的漏洞是公钥被篡改和冒充，因为大多数新手不能很快发现这一点。PGP 对该问题的解决方案是采用 CA（权威机构）认证，明确每个由其签字的公钥都被视为是真实的。这样的 CA 适合于非个人控制组织或政府机构。

现在以你和 Alice 的通信为例来理解 PGP 的公钥分发安全和认证问题。假设你想给 Alice 发封信，那你必须有 Alice 的公钥。你从 BBS 上下载了 Alice 的公钥，并用它加密了信件，再用 BBS 的 E-mail 功能将信发给了 Alice。但不幸的是，你和 Alice 都不知道有一个名为 Charlie 的用户潜入了 BBS，并将其以 Alice 名义生成的密钥对中的公钥替换了 Alice 的公钥。那么此时你用来发信的公钥就不是 Alice 的而是 Charlie 的，但一切看起来都很正常，因为你拿到的公钥的用户名是“Alice”。于是 Charlie 就可以用他手中的私钥来解密你给 Alice 的信，甚至他还可以用 Alice 真正的公钥来转发你给 Alice 的信，这样谁都不会起疑心。他如果想改动你给 Alice 的信也很容易实现。更有甚者，他还可以伪造 Alice 的签名给你或其他人发信，因为你们手中的公钥是伪造的，你们会以为真是 Alice 的来信。

防止这种情况出现的最好办法是避免让其他任何人有机会篡改公钥，比如直接从 Alice 手中得到她的公钥。然而当她远在千里之外或由于其他原因无法见面时，这是很困难的。PGP 提出了一种公钥“转介”机制来解决这个问题。比如，如果你和 Alice 有一个共同的朋友 David，而 David 知道他手中 Alice 的公钥是正确的，David 就可以用他自己的私钥在 Alice 的公钥上签名，表示他担保这个公钥属于 Alice。当然你需要用 David 的公钥来检验他给你的 Alice 的公钥，同样 David 也可向 Alice 认证你的公钥，这样 David 就成为你和 Alice 之间的“介绍人”。Alice 或 David 就可放心地把 David 签过字的 Alice 的公钥上载到 BBS 让你去拿，没人可能去篡改它而不被你发现，即使是 BBS 的管理员。这就是 PGP 利

用公共渠道传递公钥的安全手段。

由一个大家普遍信任的组织或机构担当“密钥使者”或“认证权威”，每个由它签字的公钥都被认为是真实的，这样大家只要有一份该公钥就行了。认证它的公钥也很方便，因为它广泛提供这种服务，其公钥流传广泛，因此假冒相当困难。这样的“权威”适合由非个人控制组织或政府机构充当，现在已经有等级认证制度的机构存在。

PGP 的这种密钥“转介”方式，更能反映出人们自然的社会交往，且人们也能自由地选择信任的人来介绍。这种方式是使用以个人为中心的信任模型，采用一种具有传递性的“转介信任”方式进行密钥分发的。在这种方式下，用户可以自行决定对周围的联系人是否信任及信任度的高低。用户只接收信任者传送来的公钥，并且这些公钥都带有签名。

2．私钥的管理

私钥相对于公钥而言不存在被篡改的问题，但却存在泄露的问题。对此，PGP 的办法是让用户为随机生成的 RSA 私钥指定一个口令，只有通过给出口令才能将私钥释放出来使用。用口令加密私钥的加密程序与 PGP 本身是一样的。所以，私钥的安全性问题实际上是对用户口令的保密。当然，私钥文件本身的失密也是很危险的，因为破译者只要试探出用户的口令，即可破译密钥。

PGP 在安全性问题上的精心考虑体现在其各个环节，比如每次加密的实际密钥是个随机数，PGP 程序对随机数的产生是很审慎的，关键随机数的产生是从用户看键盘的时间间隔中取得随机数种子的；采用与邮件加密同样的强度对用户磁盘上的 randseed.bin 文件进行加密，可有效地防止他人从用户的 randseed.bin 文件中分析出实际加密密钥的规律来。

小　　结

密码学是一门古老而深奥的学科，它以识别密码为本质，以加密和解密基本规律为研究对象。密码学包括密码编码学和密码分析学。

密码学的基本术语有：消息、明文、加密、密文、解密、加密算法、解密算法、密钥、密码体制。

消息是指用语言、文字、数字、符号、图像、声音或它们的组合等方式记载或传递有意义的内容。在密码学里，消息也称为信息。

明文是指未经过任何伪装或隐藏技术处理的消息。

加密是指利用某些方法或技术对明文进行伪装或隐藏的过程。

密文是指被加密的消息。

解密是指将密文恢复成原明文的过程或操作。

加密算法是指将明文消息加密成密文所采用的一组规则或数字函数。

解密算法是指将密文消息解密成明文所采用的一组规则或数学函数。

密钥是指进行加密或解密操作所需要的秘密参数或关键信息。

密码可分为手工密码、机械密码、电子机内乱密码和计算机密码、替代密码和移位密

码、保密密码和不保密密码、分组密码和序列密码、对称密钥密码和非对称密钥密码。

DES 是由 IBM 公司开发的数据加密标准，是第一个向公众公开的加密算法，也是应用最广泛的一种商用数据加密方案。DES 的算法由 64bit 的明文初始量置换 IP、乘积变换、逆初始变换 IP^{-1} 和 64bit 的密文构成。

DES 算法的特点是：具有算法容易实现、速度快、通用性强等优点；但也有密钥位数少、保密强度较差和密钥管理复杂、不便于数字签名等缺点。

DES 主要应用有：计算机网络通信、电子资金传递系统、保护用户文件和用户识别。

对称密钥密码体制在加密、解密时使用同样的密钥，这些密钥由发送者和接收者分别保存。与对称密钥密码体制不同，公开密钥密码系统采用两个不同的密钥进行加密和解密，也称“非对称式加密算法”。

最著名的公开密钥密码算法 RSA 的优点在于原理简单、易于使用、便于数字签名、可靠性较高；但也有算法复杂、加密和解密速度慢、难于用硬件实现等缺点。

将密文附在原文后，称为数字签名。

密钥管理包括密钥的产生、密钥的存储和保护、密钥的更新、密钥的分发、密钥的验证、密钥的使用、密钥的销毁等，其中最主要的是密钥的产生、保护和分发。

选用硬件加密的原因有：快速、安全和易于安装。

通信加密方式有：链路加密、节点加密和端-端加密。

链路加密指传输数据仅在数据链路层上进行加密；节点加密是为解决数据在节点中是明文的缺点而出现的一种加密方式；端-端加密是传输数据在应用层上完成加密的加密方式。

PGP 是一种广泛应用于电子邮件的加密标准，可以提供数字签名、数据加密、数据压缩和格式转换等功能。

PGP 提供的数字签名服务包括 Hash 编码或消息摘要的使用。

PGP 的数据加密通过使用对称加密算法 IDEA 对要传送的信息或在本地存储的文件进行加密。

PGP 在数字签名和加密服务之间提供压缩服务，即 PGP 先对信息进行签名，然后再进行压缩，最后对压缩的信息进行加密。

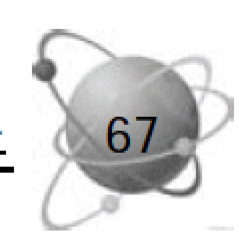
很多电子邮件只允许使用纯 ASCII 文本，为了适应这种限制，PGP 提供了将原始的 8 位数据流转换为 ASCII 字符串的服务。

练习与思考

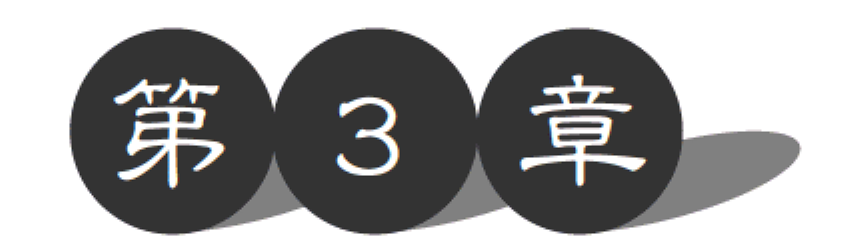
1．简述密码学两个方面的内涵。

2．试解释密码学的术语：消息、明文、加密、密文、加密算法、解密、解密算法、密钥、密码体制。

3．什么是替代密码和移位密码？举例说明。



4．试解释保密密码和不保密密码的内涵。
5．什么是分组密码和序列密码？
6．什么是一次一密钥密码？举例说明。
7．简述数据加密标准 DES 的特点及应用。
8．简述 RSA 算法的特点及应用。
9．对称密码系统的安全性依赖于哪两个因素？
10．数字签名为何能有与手写签名一样的作用？
11．TCP/IP 服务存在哪些安全缺陷？
12．为什么通信加密的硬件加密很受商业和军事等领域青睐？
13．简述链路加密和端-端加密的特点。
14．简述 PGP 软件的功能。
15．PGP 软件可应用在什么场合？
16．PGP 软件如何实现私钥的管理？



网络操作系统安全

本章学习要求：

（1）掌握访问控制的概念及其措施。
（2）掌握 Windows NT 操作系统的安全技术及安全管理措施。
（3）掌握 Windows NT 操作系统数据的安全管理。
（4）了解网络操作系统安全的概念。
（5）了解访问控制的类型。
（6）了解 UNIX/Linux 操作系统安全。

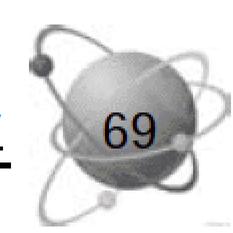
重点和难点：

（1）重点：Windows NT 操作系统的安全技术、安全管理措施及数据的安全管理。
（2）难点：Windows NT 操作系统的安全技术、UNIX/Linux 操作系统安全。

网络操作系统是网络资源的协调者和管理者，网络上的服务器软件都是运行在网络操作系统上的，所以网络操作系统是整个信息系统安全的基础。没有网络操作系统的安全，就没有主机和网络资源的安全。本章主要介绍网络操作系统安全的基础知识，并对 Windows NT、UNIX 及 Linux 的网络安全管理的技术、安全措施和安全配置进行介绍。

3.1 网络操作系统的概念

网络操作系统（Network Operation System，NOS）是向网络计算机提供网络通信和网络资源共享功能的操作系统，由一系列负责管理整个网络资源和方便网络用户使用的软件组成，是整个网络的灵魂。网络设备，例如路由器、交换机的主要功能是把整个网络连接起来，让网络各节点之间可以互相通信，而网络操作系统的主要功能则是管理网络中的资源，并向网络中的用户提供各种网络服务。NOS 除了具有普通操作系统所具有的进程控制与调度、信息处理、处理机管理、存储器管理和设备管理等功能外，还提供了高效而可靠



的网络通信环境与多种网络服务，如分布式文件共享、网络打印服务、数据库服务、域名解析服务和 Web 服务等。

网络操作系统支持不同的网络硬件环境；支持多个服务器，可实现服务器之间透明地进行管理信息的传递；在多用户环境下，支持多用户对网络的使用；桥接能力——在同一个网络操作系统下，支持具有多种不同硬件和底层通信协议的网络协同工作；支持系统备份、安全性管理、容错和性能控制；安全性和接入控制：通过对用户和资源的控制，来保证网络的安全性；为用户提供与网络的交互接口。

目前，常用的网络操作系统有 Windows Server、UNIX、Linux、NetWare。

1. Windows Server

微软公司的 Windows 系统不仅在个人操作系统方面占有绝对优势，在网络操作系统中也具有非常高的市场占有率。常见的 Windows 网络操作系统有 Windows Server 2008、Windows Server 2003、Windows 2000 Server 及 Windows 2000 Advance Server。如果说 Windows 2000 Server 全面继承了 NT 技术，那么 Windows Server 2003 则是依据.NET 架构对 NT 技术作了重大的发展和实质性改进，凝聚了微软多年来的技术积累。Windows Server 2003 在各行业及政府机构中已经得到了广泛的应用，而最新的版本 Windows Server 2008 也已经正式发布。

2. UNIX

UNIX 是一个强大的多用户、多任务操作系统，支持多种处理器架构，最早由 Ken Thompson、Dennis Ritchie 和 Douglas Mcilroy 于 1969 年在 AT&T 的贝尔实验室开发。这种网络操作系统稳定性和安全性非常好，但由于其操作界面没有 Windows 系统那么友好，多数的操作都是使用命令行的方式来完成，不容易掌握，因此小型局域网和小企业中基本不使用 UNIX 作为网络操作系统，而一般用于大型的网站或大型的企业中。目前常见的 UNIX 系统有：SUN 的 Solaris、IBM 的 AIX 和惠普的 HPUNIX 等。

3. Linux

Linux 是由芬兰赫尔辛基大学的学生 Linus Torvalds 在 1992 年首创的。Linux 是一套免费使用和自由传播的类 UNIX 操作系统。我们通常所说的 Linux，指的是 GNU/Linux ，即采用 Linux 内核的 GNU 操作系统。Linux 从 Internet 服务器到用户的桌面，从图形工作站到 PDA 的各种领域都得到了广泛的应用。目前有许多的 Linux 发行版可供人们选择使用，其中常见的中文 Linux 发行版本有 RedHat（红帽子）、红旗 Linux 和 TurboLinux 等。

4. NetWare

NetWare 是 Novell 公司推出的网络操作系统。NetWare 最重要的特征是基于基本模块设计思想的开放式系统结构。NetWare 是一个开放的网络服务器平台，可以方便地对其进行扩充。NetWare 曾风行全球，占据了 LAN 的大部分市场，但在 Windows NT 操作系统出现之后，NetWare 的大部分市场已被 Windows NT 抢占。到目前为止，仍有一定数量的用户使用 NetWare 操作系统。

网络操作系统在网络应用中发挥着十分重要的作用，因此网络操作系统本身的安全就成为了网络安全保护中的重要内容。

3.2 操作系统的安全与访问控制

操作系统负责对计算机系统的各种资源、操作、运算和计算机用户进行管理与控制，它是计算机系统安全功能的执行者和管理者，是所有应用软件的运行基础。没有操作系统提供的多种安全机制，数据库、网络和其他应用软件的安全问题将不可能从根本上解决，信息安全只能是“沙地上的堡垒”。

威胁操作系统资源安全的因素除设备部件故障外，还有以下几种。

- 对系统的不合理配置或用户的误操作，造成对资源违反意愿的处理。例如，无意中删除文件或更改文件的访问控制权限等。
- 恶意用户非法获取对资源访问的权限。例如，计算机“黑客”窃取其他用户的秘密或不想共享的信息。窃取的方法有多种，可以通过破解其他用户的口令来获取该用户的资源，或者通过执行暗藏在正常程序中的“特洛伊木马”程序秘密窃取其他用户在内存或外存上的信息。
- 恶意破坏系统资源或系统的正常运行。例如，拒绝服务攻击和计算机病毒。
- 多用户操作系统还需要防止各用户程序在执行过程中相互干扰。

3.2.1 操作系统安全的概念

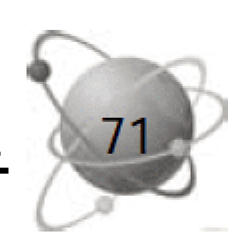
操作系统安全是指该系统能够控制外部对系统信息的访问，即只有经过授权的用户或进程才能对信息资源进行相应的读、写、创建和删除等操作，以保护合法用户对授权资源的正常使用，防止非法入侵者对系统资源的侵占和破坏。

对网络操作系统的安全保护应包含以下几个方面。

- 对操作系统本身的安全保护功能和安全服务。
- 针对各种常用的操作系统，进行相应配置，使之能正确应对和防御各种入侵。
- 保证网络操作系统本身所提供的网络服务能得到安全配置。

操作系统不但要强调安全性，还要强调对硬件和应用软件有良好的兼容性。一个完全封闭的系统，也许在系统安全上很优秀，但是只能运行在特定的硬件环境上，只能运行少数应用程序，甚至只有少数的用户才能使用系统的资源，那么这种系统安全的通用性意义不大。

操作系统安全机制主要包括隔离控制和访问控制。隔离控制主要有物理设备或部件隔离、时间隔离、逻辑隔离和加密隔离等实现方法；而访问控制是操作系统中最有效、最直接的安全措施，是操作系统安全机制的关键。



3.2.2　访问控制的概念及含义

访问控制是在身份认证的基础上，根据用户身份对提出的资源访问请求加以控制，是针对越权使用资源的现象进行防御的措施。访问控制具体包括两个方面的含义：一是指用户的身份验证即对用户进入系统的控制，最简单常用的方法是用户账户与口令验证；二是用户进入系统后根据用户的身份对其访问资源的行为加以限制，最常用的方法是访问权限和资源属性限制。访问控制在整个信息安全系统的逻辑结构中所处的位置如图 3-1 所示。

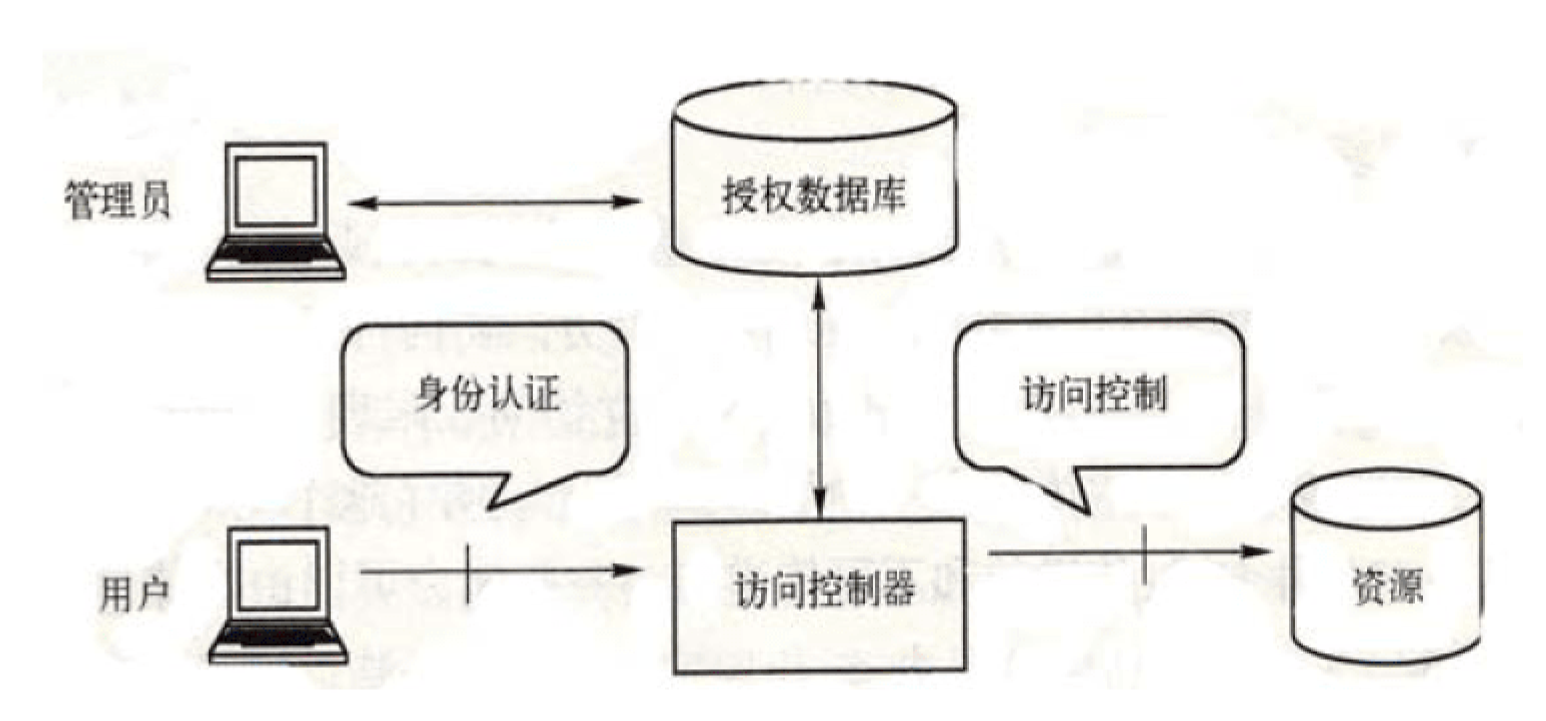


图 3-1　信息安全系统的逻辑结构

在访问控制系统中，一般包括主体、客体和访问策略 3 个要素。

（1）主体是指发出资源访问操作请求的主动方，是动作的发起者。主体的含义是广泛的，可以是用户组、用户本身，也可以是用户使用的计算机终端、移动设备等，甚至可以是网络上的硬件设备、无线通信中的终端等。

（2）客体是接受其他实体访问的被动方，是在访问中必须进行控制的资源。凡是可以被操作的数据、对象都可以认为是客体。客体可以是数据、文件、信息等的集合体，也可以是网络上的硬件设备、无线通信中的终端等。

（3）访问策略就是一套访问的规则，用以确定一个主体是否对客体拥有访问的能力。它决定了主体与客体之间交互作用时可行的操作。

访问控制的目的是为了限制主体对客体的访问权限，决定用户能做什么操作，也决定了应用程序可以进行什么样的操作，从而使资源在合法的范围内使用。

3.2.3　访问控制的类型

访问控制依其不同的实现方法，可以分为自主访问控制、强制访问控制、基于角色的访问控制、基于任务的访问控制和基于对象的访问控制等。

1. 自主访问控制

自主访问控制（Discretionary Access Control，DAC）是一种最为普遍的访问控制手段，是指系统允许经过身份验证和授权之后，有访问许可的主体能够直接或间接地向其他主体

转让访问权。自主访问控制是在确认主体身份以及（或）它们所属组的基础上，控制主体的活动，实施用户权限管理、访问属性（读、写、执行）管理等。

自主访问控制的特点是主体可以自主地把自己所拥有客体的访问权限授予其他主体或者从其他主体收回所授予的权限，访问通常基于访问控制表（Access Control List，ACL）。

2．强制访问控制

强制访问控制（Mandatory Access Control，MAC），是用户和客体资源都被赋予了一定的安全级别，用户不能改变自身和客体的安全级别，只有管理员才能确定用户和用户组的访问权限。

强制访问控制一般与自主访问控制结合使用，并且实施一些附加的、更强的访问限制。一个主体只有通过了自主与强制性访问限制检查后，才能访问某个客体。用户可以利用自主访问控制来防范其他用户对自己客体的攻击。由于用户不能直接改变强制访问控制属性，所以强制访问控制提供了一个不可逾越的、更强的安全保护层以防止其他用户偶然或故意地滥用自主访问控制。

自主访问控制和强制访问控制在企业的组织结构或者是系统安全需求处于变化的过程中，需要大量的、繁琐的授权变动，系统管理员的工作将变得非常繁重，更糟糕的是容易发生错误造成一些意想不到的安全漏洞。因此，有必要引入其他的访问控制方法来加以解决。

3．基于角色的访问控制

基于角色的访问控制（Role-Based Access Control，RBAC）的基本思想就是要求确定每一个用户在系统中所扮演的角色，不同的角色具有不同的访问权限，这些权限由系统管理员分配给角色，用户可执行的操作与其所扮演角色的职能相匹配。

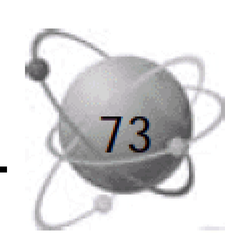
RBAC 从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色相联系。例如，角色“数据备份管理员”的权限就是只能完成对系统数据的备份和还原的相关操作。通过给用户分配合适的角色，让用户与访问权限相联系，使角色成为访问控制中访问主体和客体之间的一座桥梁。

RBAC 中引入了角色的概念，用角色表示访问主体具有的职权和责任，灵活地表达和实现了企业的安全策略，使系统权限管理在企业的组织视图这个较高的抽象集上进行，从而简化了权限设置，较好地解决了企业管理信息系统中用户数量多、变动频繁的问题。

4．基于任务的访问控制

基于任务的访问控制（Task-Based Access Control，TBAC）是从应用和企业层角度来解决安全问题，而已往的访问控制是从系统的角度出发。它采用“面向任务”的观点，从任务的角度来建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。

在 TBAC 中，对象的访问权限控制并不是静止不变的，而是随着执行任务的上下文环境发生变化，这也正是我们称其为主动安全模型的原因。TBAC 是在工作流的环境中考虑



对信息的保护问题。在工作流环境中，每一步对数据的处理都与以前的处理相关，相应的访问控制也是这样，因而 TBAC 是一种上下文相关的访问控制模型。它不仅能对不同工作流实行不同的访问控制策略，而且还能对同一工作流的不同任务实例实行不同的访问控制策略。这就是"基于任务"的含义，所以 TBAC 又是一种基于实例（Instance-Based）的访问控制模型。由于任务都有时效性，所以在基于任务的访问控制中，用户对于授予他的权限的使用也是有时效性的。

5. 基于对象的访问控制

基于对象的访问控制（Object-Based Access Control，OBAC）是一种基于受控对象的访问控制方法。它将访问控制列表与受控对象或受控对象的属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合；同时允许对策略和规则进行重用、继承和派生操作。这样，不仅可以对受控对象本身进行访问控制，对受控对象的属性也可以进行访问控制，而且派生对象可以继承父对象的访问控制设置，这对于信息量巨大、信息内容更新变化频繁的管理信息系统非常有益，可以减轻由于信息资源的派生、演化和重组等带来的分配、设定角色权限等的工作量。

OBAC 从信息系统的数据差异变化和用户需求出发，有效地解决了信息数据量大、数据种类繁多、数据更新变化频繁的大型管理信息系统的安全管理问题。OBAC 从受控对象的角度出发，将访问主体的访问权限直接与受控对象相关联，一方面定义对象的访问控制列表，增加、删除、修改访问控制项易于操作；另一方面，当受控对象的属性发生改变，或者受控对象发生继承和派生行为时，无须更新访问主体的权限，只需要修改受控对象的相应访问控制项即可，从而减少了访问主体的权限管理，降低了授权数据管理的复杂性。

3.2.4　访问控制措施

访问控制是保证网络系统安全的主要措施，其主要任务是保证网络资源不被非法使用和非法访问。具体的访问控制措施有以下几种：

1. 入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站上入网。用户的入网访问控制可分为 3 个步骤：用户名的识别与验证、用户口令的识别与验证、用户账户的默认限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。每个用户在网络注册时都要由系统指定或由用户自己选择一个用户账户和用户口令，这些账户和口令均会存放在特定的数据库中。用户在接入网络时首先要输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才继续验证用户输入的口令；否则，用户将被拒之于网络之外。用户的口令是用户入网的关键所在。为保证口令的安全性，用户口令必须经过加密，然后存储到特定的数据库中。

除了采用用户名和口令进行验证之外，也可利用生物识别技术对用户进行唯一特征（例如，指纹、声音、视网膜图像等）的验证，还可以使用便携式验证器，如智能卡、加密狗等硬件来验证用户的身份。

用户名和口令验证有效之后，再进一步进行用户账户的默认限制检查。系统应能控制用户登录入网的站点、限制用户入网的时间、限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时，网络还应能对用户的账户加以限制，用户此时将无法进入网络访问网络资源。此外，系统还应对所有用户的访问进行审计，包括用户的访问时间及访问行为。

为了防止非法用户使用暴力破解的方式（即采用穷举的方式）破解正常用户的账户和密码，系统在用户登录时应制定账户锁定策略。在达到最大的登录失败次数之后，系统将自动锁定该账户，不允许该账户反复尝试登录系统。

2. 资源访问控制

资源访问控制是对客体资源信息的访问控制管理，其中包括系统访问控制、文件目录访问控制和文件属性访问控制。

- 系统访问控制是指一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。应限制普通用户对服务器控制台的访问，以防止非法用户修改、删除服务器的配置；并做好服务器操作的审计工作，记录用户对服务器配置的修改。
- 文件目录访问控制是指用户被赋予一定的权限，在权限的允许下，哪些用户可以访问哪些目录、子目录、文件和其他的资源，哪些用户可以对其中的哪些目录、子目录、文件或设备进行哪些操作。
- 属性是系统直接赋予文件和目录等资源的，对所有用户都具有约束权。文件属性访问控制将给定的属性与网络服务器的文件、目录和网络设备联系起来，在权限安全的基础上提供了更进一步的安全性。一旦目录、文件具有了某些属性，用户（包括系统管理员）便不能超越这些属性规定的访问权，即不论用户的访问权限如何，只能按照资源的属性实施访问。

3. 网络服务器安全控制

网络服务器允许用户以远程控制台或远程登录的方式来进行服务器的设置。用户使用控制台可以装载和卸载模块，进行安装和删除软件等操作。网络服务器的安全控制包括设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；设定服务器登录的时间限制、非法访问者检测和关闭的时间间隔等。

4. 网络端口和节点的安全控制

网络中的节点和端口经常用于加密传输数据和进行数据的安全路径选择，这些重要的位置必须能够抵御黑客的攻击。访问网络重要端口和节点时，要求访问者必须提供足以证明其身份的标识。

5．网络监测和锁定控制

网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问。对非法的网络访问，服务器应以图形、文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

6．防火墙控制

防火墙（Firewall）是在两个网络之间执行访问控制策略的一个或一组安全系统。它是一种计算机硬件和软件系统的集合，是实现网络安全策略的有效工具之一。通常防火墙建立在内部网和 Internet 之间的一个路由器或计算机上。它就如同一堵带有安全门的墙，可以阻止外界对内部网资源的非法访问和通行合法访问，也可以防止内部对外部网的不安全访问和通行安全访问。

3.3　Windows NT 系统安全

Windows NT 是 Microsoft 推出的面向工作站、网络服务器和大型计算机的网络操作系统，也可用作 PC 机操作系统。它与通信服务紧密集成，提供文件和打印服务，能运行客户机/服务器应用程序，内置了 Internet/Intranet 功能，已逐渐成为企业组网的标准平台。NT 即新技术（New Technology），从 5.0 版开始 Windows NT 只是简单地称为 Windows。下面的讲解将以介绍 Windows Server 2003（Windows NT 5.2）为主。

3.3.1　Windows NT 的安全基础

Windows NT 提供了两个微软管理界面 MMC 的插件作为安全性配置工具，即安全性模板和安全性配置分析。安全性模板提供了针对 10 多种角色（从基本工作站、基本服务器一直到高度安全的域控制器）的计算机的管理模板，这些角色的安全性要求是不同的。通过安全性配置，管理员可以创建针对当前计算机的安全性策略。以下是 Windows NT 系统的安全特性。

1．数据的安全性

Windows NT 所提供的保证数据保密性和完整性的特性，主要体现在以下 3 个方面。

（1）用户登录的安全性。从用户登录网络开始，Windows NT 借助 Kerberos 和 PKI 等验证协议提供了强有力的口令保护和单点登录。

（2）网络数据的保护。本地网络中的数据是由验证协议来保证其安全性的。如果需要更高的安全性，还可以通过 IPSec 的方法，提供点到点的数据加密安全性。

（3）存储数据的保护。可以采用数字签名来签署软件产品或者加密文件系统。加密文件系统对每个文件都采用随机密钥来加密，不但可以加密本地的 NTFS 文件或文件夹，还可以加密远程的文件，不影响文件的输入/输出。其恢复策略由 Windows NT 的整体安全性

策略决定，具有恢复权限的管理员才可以恢复数据，但是不能恢复用来加密的密钥。

2．企业之间通信的安全性

Windows NT 为不同企业之间的通信提供了多种安全协议和用户模式的内置的集成支持，其实现方式如下。

（1）在目录服务中创建专门为外部企业开设的用户账号。通过 Windows NT 的活动目录，可以设定组织单元、授权或 VPN 等方式，并对它们进行管理。

（2）建立域之间的信任关系。用户可以在 Kerberos 认证或 PKI 得到验证之后，远程访问已经建立信任关系的域。

（3）公用密钥体制及电子证书可以用于提供用户身份确认和授权，企业可以把通过电子证书的外部用户映射为目录服务中的一个用户账号。

3．企业和 Internet 的单点安全登录

当用户成功地登录到网络之后，Windows NT 透明地管理一个用户的安全属性，而不管这种安全属性是通过用户账号和用户组的权限规定来体现的，还是通过数字签名和电子证书来体现的。先进的应用服务器都应该能从用户登录时所使用的安全支持提供器接口（Security Support Provider Interface，SSPI）获得用户的安全属性，从而使用户做到单点登录，访问所有的服务。

4．安全管理的易操作性和良好扩展性

通过在活动目录中使用组策略，管理员可以集中地把所需要的安全保护加强到某个计算机对象上。Windows NT 包括了一些安全性模板，既可以针对计算机所担当的角色来实施，也可以作为创建定制的安全性模板的基础。

3.3.2 Windows NT 安全漏洞的修补

Windows 系统存在着很多安全漏洞，黑客们往往利用这些漏洞进行攻击。虽然防火墙可起到一定的防护作用，但是有些破坏性程序仍然可以利用系统漏洞绕过防火墙入侵系统。对于系统漏洞，最好的解决方法是打补丁或者软件修补。

微软在其网站上不定期地发布安全更新公告，周期大约为每个月两次。中文公告的地址为 http://www.microsoft.com/china/technet/security/current.mspx。为了让用户知道在什么时候进行安全更新，微软制定了对个人安全升级的一个风险级别指标。微软的风险级别是根据国际标准化组织 ISO 的风险管理级别制定的。这些级别推荐我们何时需要安装安全更新，如表 3-1 所示。

表 3-1 微软安全风险级别

严重级别	定义	建议升级时间
紧急	系统可以让某些蠕虫病毒在没有用户行为的情况下进行繁殖	在 24 小时之内
重要	系统可以采取折中的办法来平衡用户数据的机密性、完整性、有效性与处理资源的完整性和有效性之间的关系	在 1 个月之内

续表

严 重 级 别	定　　义	建议升级时间
一般	情况严重，但是已经被化解为一个可以容忍的程度。可通过修改默认配置、审核用户行为来提高系统的安全性	等到下一个升级包出现，或者最迟在 4 个月之内升级
低风险	黑客利用该漏洞攻击的难度很大或只会产生很轻微的影响	等到下一个升级包出现，或者最迟在 1 年之内升级

如果想查看系统缺失的安全更新补丁和潜在漏洞，可以使用微软基准安全分析工具（Microsoft Baseline Security Analyzer，MBSA）。MBSA 包括可执行本地或远程 Windows 系统扫描的图形和命令行界面，其图形界面如图 3-2 所示。MBSA 将扫描基于 Windows 的计算机，并检查操作系统和已安装的其他组件（如 IIS（Internet Information Services）和 SQL Server），以发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。MBSA 需要以管理员权限开启特定的服务，才能对目标主机进行扫描。例如，MBSA 需要开启目标主机的 Server 服务和远程注册服务。

MBSA 是微软的免费工具，可以登录 http://www.microsoft.com/china/technet/security/tools/mbsahome.mspx 下载。

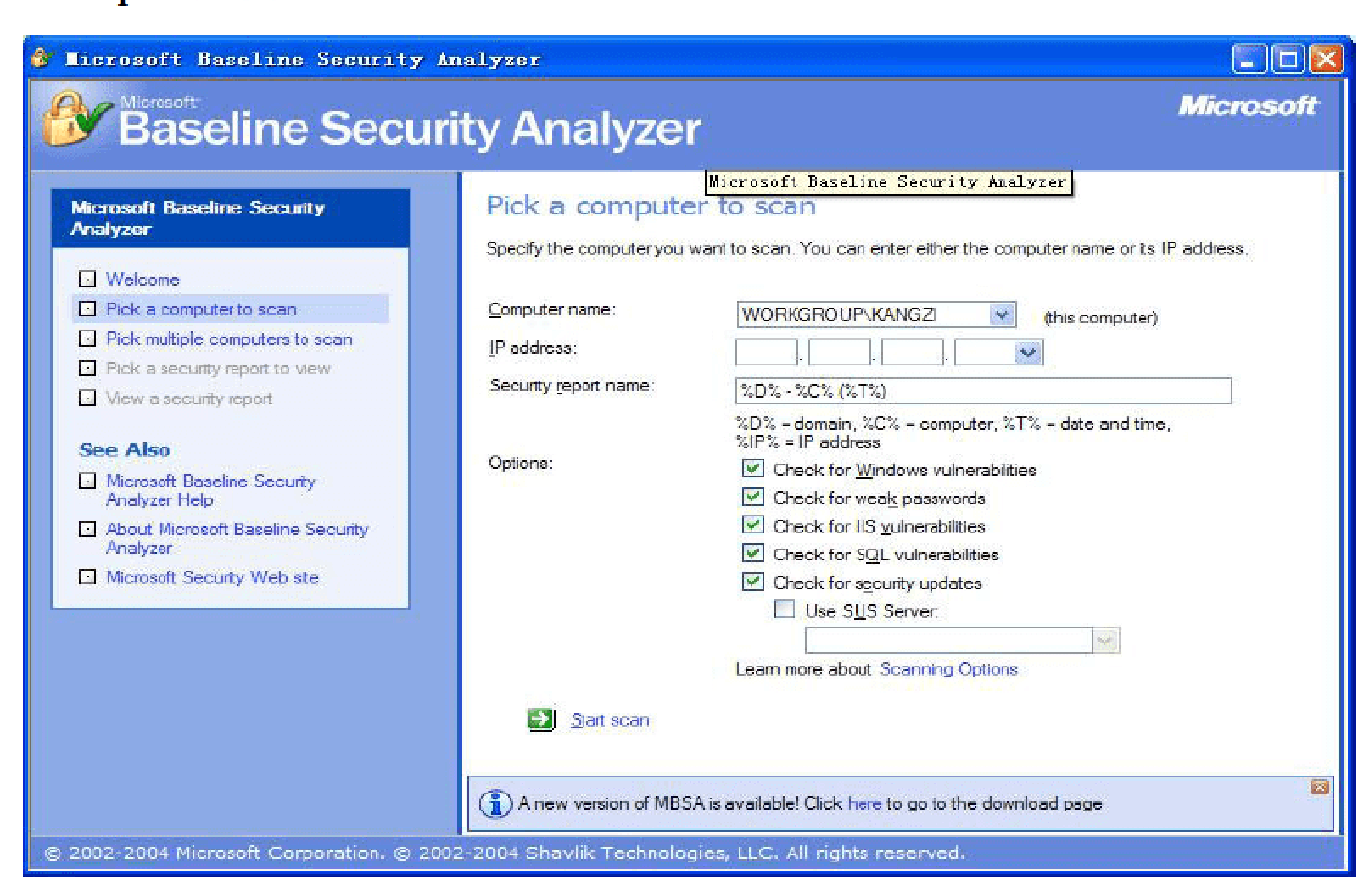


图 3-2　MBSA 的图形界面

微软安全更新的安装方式有以下 3 种：

1．Windows 自动更新

对终端用户而言，最好的安全更新方式就是让他们根本不需要考虑这个问题。Windows 的自动更新就是专门针对这种情况设计的。当有新的 Windows 安全更新时可以自动通知用户，并且可以配置自动下载和安装哪些更新。用户不以管理员身份登录，更新功能仍起作用。如果安装更新需要重新启动，则 Windows 会自动地重启计算机。这个特性使自动更新很少运用在服务器上。

在安装好操作系统之后第一次启动时，机器会询问是否激活自动更新。默认选项是马

上下载所有的补丁，并通知用户进行安装。

2. Windows 软件更新服务

对于中小型网络，最好的选择可能是配置所有的客户机为自动更新，而服务器使用手动更新，然而某些用户可能需要定制安全更新或者需要特定应用程序的更新，此时 Windows 软件更新服务（Windows Software Update Services，WSUS）便派上了用场。WSUS 可以从微软网站上免费下载，用户可以拥有自己的 Windows 更新服务器。不同点是 Windows 自动更新为用户提供了所有可用的安全更新，而 WSUS 只限于用户所需要的安全更新。如果用户配置了一台 WSUS 服务器，就能配置每一台计算机需要的更新，以确保所有客户机安装指定的更新，而不安装其他任何更新。配置 WSUS 还可以减少网络负载，满足特殊部门的需要。

3. 微软的系统管理服务器

微软的系统管理服务器（Systems Management Server，SMS）为 Microsoft 平台提供了用于更新及配置管理的全面解决方案，从而确保企业能迅速为用户提供相关的软件和更新。SMS 系统功能非常强大，除了安全补丁管理功能之外，还集成了应用系统部署、资产管理和 Windows 管理服务集成等功能，适合于大型企业使用。

3.3.3 Windows NT 的安全机制和技术

1. Windows NT 的安全机制

Windows NT 操作系统不仅通过新的网络技术来协助组织扩展其操作，也通过增强的安全性服务来协助组织保护其信息及网络资源。Windows 分布式安全服务主要针对以下业务需求：让用户登录一次即可访问所有企业资源的能力；强大的用户身份验证及授权能力；内部和外部资源间的安全通信；设置及管理必要安全性策略的能力；自动化的安全性审核；与其他操作系统和安全协议的互操作性；支持使用 Windows 安全设置功能进行应用程序开发的可扩展架构。这些功能是整体 Windows 安全设置架构的重要元素。Windows NT 的操作系统安全级别为 C2，主要包含安全策略、用户验证、访问控制、加密、审计和管理这六大安全机制。Windows NT 安全系统的逻辑结构如图 3-3 所示，其中最主要的是身份验证机制和访问控制机制。

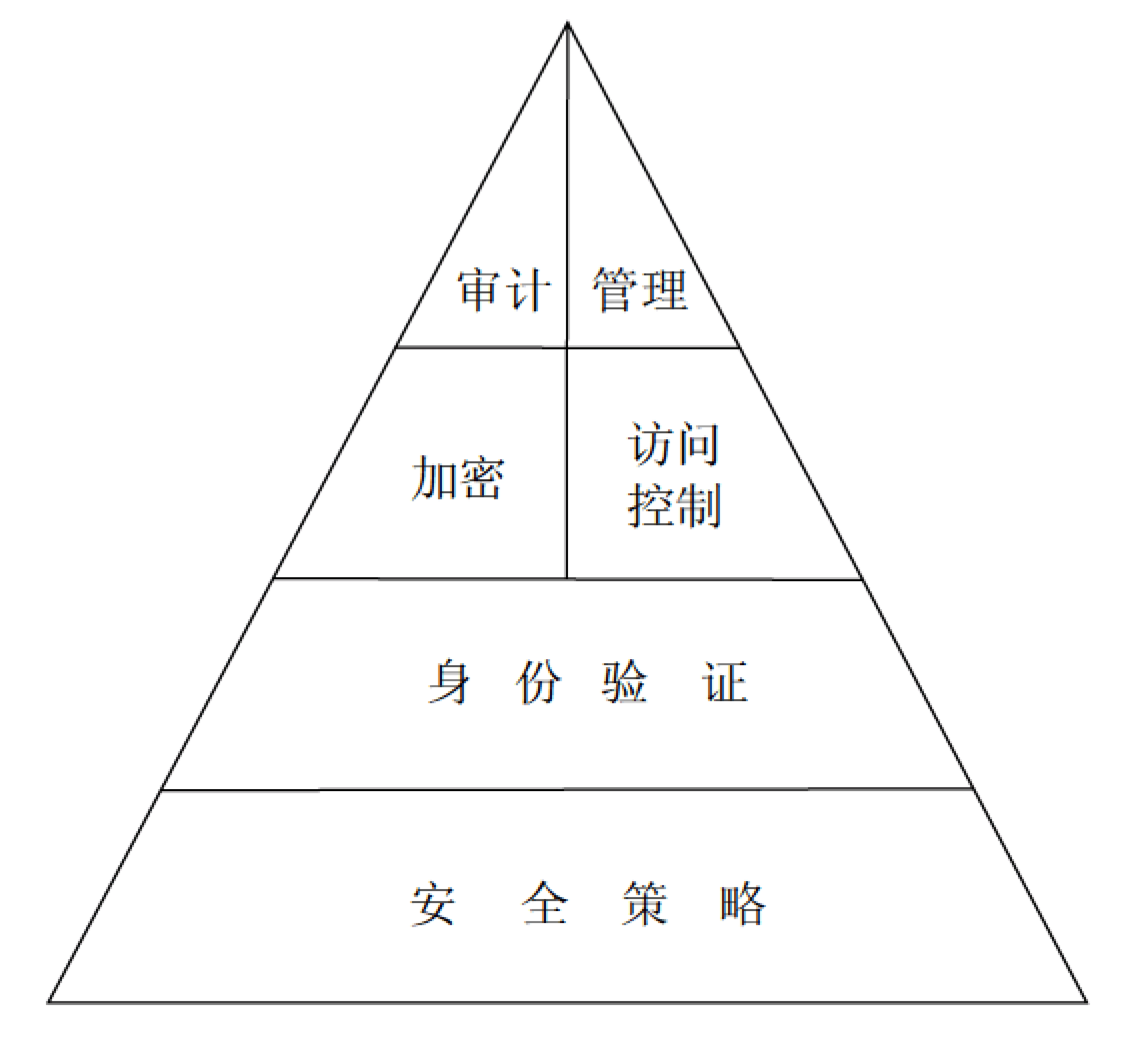


图 3-3 Widnows NT 安全系统的逻辑结构

（1）用户身份验证

Windows NT 的安全模型包括用户身份验证的概念，这种身份验证赋予用户登录系统访问网络资源的能力。在这种身份验证模型中，安全性系统提供了两种类型的身份验证，即

交互式登录和网络身份验证。为了提供这两种类型的身份验证，Windows NT 安全系统包括了 3 种不同的身份验证机制——Kerberos V5、公钥证书和 NTLM（NT LAN Manager）因为第一次出现 NTLM 缩写，所以要加上原词。用户在活动目录中必须有一个 Windows 用户账户，以登录到计算机或域中。此账户会为用户创建一个身份，然后操作系统会使用此身份验证用户的身份并授予访问特定域资源的权限。用户账户还可用作一些应用程序的服务账户。也就是说，服务可被配置成以用户账户登录（身份验证），然后通过该用户账户授予对特定网络资源的访问权限。

（2）基于对象的访问控制

通过用户身份验证，Windows 允许管理员控制网上资源或对象的访问。管理员通过对存储在活动目录中的对象进行安全设置可以实现对网上资源的访问控制。文件、打印机和服务等在活动目录中都是对象的实例。通过管理对象的属性，管理员可以设置权限，分配所有权以及监视用户访问。管理员不仅可以控制对特殊对象的访问，也可以控制对该对象特定属性的访问。

2. Windows NT 的安全技术

（1）活动目录和域

活动目录用于存储整个网络上资源的目录信息，便于用户快速、准确地查找、管理和使用这些资源。活动目录提供了目录服务功能，其中就包括集中组织、管理和控制网络资源访问的方法。活动目录使物理网络拓扑和协议透明化，这样网络上的用户可以访问资源，而不需要知道资源在什么地方，或物理上它是如何连接到网络上的。同时，活动目录提供了对网络资源的集中控制，允许用户只登录一次就可以访问整个活动目录的资源。

Windows NT 的安全机制是建立在对象的基础上的，因此对象的概念与安全问题密切相关。活动目录中存储网络对象的信息。活动目录对象代表网络资源，例如用户、组、计算机和打印机，而且网络中所有的服务器、域和站点都作为对象。

域是活动目录中逻辑结构的核心单元。一个域包含许多台计算机，它们由管理者设定，共用一个目录数据库。每一个域都有一个唯一的名称。在 Windows NT 网络中，域起着安全边界的作用——保证域的管理者只能在该域内有必要的管理权限，除非管理者获得其他域的明确授权。每个域都有自己的安全策略和与其他域的安全联系方式。

信任关系是域与域之间建立的连接关系。它可以执行对经过委托的域内用户的登录审核工作。域之间经过委托后，用户只要在某一个域内有一个用户账户，就可以使用其他域内的网络资源了。

Windows NT 系统提供 4 种基本的域模型：单域模型、主域模型、多主域模型和完全信任域模型。

① 单域模型：网络中只有一个域，就是主域，域中有一个主域控制器和一个或多个备份域控制器。该模型适用于用户较少的网络。

② 主域模型：网络中至少有两个域，但只在其中一个域（主域）中创建所有用户并存储这些用户信息。其他域则称为资源域，负责维护文件目录和打印机资源，但不需要维护用户账户。资源域都信任主域，使用主域中定义的用户和全局组。该模型适用于用户不太

多，但又必须将资源分组的情况。

③ 多主域模型：网络中有多个主域和多个资源域，其中主域作为账户域，所有的用户账户和组都在主域之上创建。各主域都相互信任，其他的资源域都信任主域，但各资源域之间不相互信任。该模型便于大型网络的统一管理，具有较好的伸缩性。因此，该模型适用于用户数很多且有一个专门管理机构的网络。

④ 完全信任域模型：网络中有多个主域，且这些域都相互信任；所有域在控制上都是平等的，每个域都执行自己的管理。该模型适用于各部门管理自己的网络。

（2）Kerberos 验证协议

Kerberos 是由 MIT 开发的用于提供网络认证服务的系统。它可用来为网络上的各种 Server 提供认证服务，使得口令不再是以明文方式在网络上传输，并且连接之间的通信是加密的。它和 PKI 认证的原理不同，PKI 使用公钥体制（不对称密码体制），Kerberos 基于私钥体制（对称密码体制）。Kerberos 称为可信的第三方验证协议，意味着它运行在独立于任何客户机或服务器的服务器之上。Kerberos 5 的身份验证协议提供了一种相互验证（通过服务器和客户端相互验证或者一台服务器与其他服务器之间相互验证）的身份验证机制。Kerberos 为远程登录提供安全性并可提供单个登录解决方案，以便用户无须每次访问新服务器时都登录。验证服务器将所有用户的密码存储在中央数据库中，由它颁发凭据，而客户端使用凭据来访问验证服务器领域内的服务器。适用范围包括接入服务器跟踪的所有用户和服务器。验证服务器由一个管理人员在物理上进行保护和管理。由于它验证用户身份，因此应用程序服务器得以免除此任务，它们“信任”验证服务器为特定客户颁发的凭据。Kerberos 系统对用户的口令进行加密后作为用户的私钥，避免了口令在信道中的明文传输，实现了较高的安全性；用户在使用过程中，仅在登录时要求输入口令，实现对合法用户的透明性。Kerberos 还可以较方便地实现用户数的动态改变。Kerberos 协议已被完全集成到 Windows NT 5.0 的安全性结构中。

（3）加密文件系统 EFS

对受保护文件的访问，可以通过用户权限来限制。然而，如果入侵者能够得到用户对磁盘驱动器的权限，即可在其他计算机上安装该驱动器，然后在该机的操作系统平台上用管理级特权访问存储在该驱动器上的数据。为了防止这种情况的发生，Windows NT 提供了一种解决方案——数据加密。数据加密使用一种称为“加密文件系统（Encrypting File System，EFS）”的功能。在 Windows NT 的 NTFS 文件系统中内置了 EFS 加密系统，利用 EFS 加密系统可以对保存在硬盘上的文件进行加密。EFS 加密系统作为 NTFS 文件系统的一个内置功能，其加密和解密过程对应用程序和用户而言是完全透明的。另外 Windows NT 内置了数据恢复功能，可以由管理员恢复被另一个用户加密的数据，保证了数据在需要使用的情况下始终可用。

EFS 对 NTFS 卷上的文件和数据，都可以进行直接的操作系统加密保存，在很大程度上提高了数据的安全性。EFS 加密是基于公钥策略的。在使用 EFS 加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的文件加密钥匙（File Encryption Key，FEK），然后将利用 FEK 和数据扩展标准 DES 算法创建加密后的文件，并把它存储到硬盘上，同时

删除未加密的原始文件。随后系统利用用户的公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时，系统首先利用当前用户的私钥解密 FEK，然后利用 FEK 解密出文件。在首次使用 EFS 时，如果用户还没有公钥/私钥对（统称为密钥），则会首先生成密钥，然后加密数据。如果用户登录到了域环境中，密钥的生成依赖于域控制器，否则它就依赖于本地机器。

EFS 加密机制和操作系统紧密结合，这样也就不必为了加密数据而安装额外的软件，节约了使用成本。EFS 加密系统对用户是透明的，也就是说，如果用户加密了一些数据，那么该用户对这些数据的访问将是完全允许的，不会受到任何限制。而其他非授权用户试图访问加密过的数据时，就会收到“访问拒绝”的错误提示。EFS 加密的用户验证过程是在登录 Windows 时进行的，只要登录到 Windows 就可以打开任何一个被授权的加密文件。

（4）安全性支持——Windows IP Security

绝大多数的网络管理员在考虑网络安全性时，都把重点放在如何防止从企业网络外部发起的攻击，防火墙、安全路由器、拨号访问的令牌验证等概念也就出现了。这些措施无疑大大增强了企业网络的周围防线，但所有这些都不能杜绝来自企业网内部的攻击。很多重要机密信息的泄露与遗失往往是由于企业雇员、技术支持人员或临时合同工从内部侵入公司网络造成的。

为了解决以上问题，Windows NT 5.0 推出了一种新的网络安全性方案——IP Security，简称 IPSec。它符合 IETF 宣布的 IP 安全性协议的标准，支持在网络层一级的验证、数据完整性和加密。IPSec 的主要目的是为 IP 数据包提供保护。IPSec 的基础是端-端的安全性模型，也就是说只有发送者和接收者这两台主机知道有关 IPSec 保护的情况。各个计算机都在它自己的一端处理安全性。

在进行数据交换之前，先相互验证计算机，在两个计算机之间建立安全性协作关系。在数据传输之前，加密要传输的数据。在鉴别或者加密数据时，IPSec 采用标准的 IP 数据包格式。因此，中间的网络设备没有必要用不同于标准 IP 数据包的方法来处理 IPSec 数据包。IP Security 存在于传输层之下，因此它对应用程序和用户来说都是透明的。也就是说，当在防火墙和路由器上实现 IP Security 时，用户桌面的网络应用程序不需要做任何修改。

3.3.4　Windows NT 的安全管理措施

1. 物理安全

服务器应当放置在安装了监视器的隔离房间内，并且应当保留 15 天以内的监控录像记录；机箱、键盘、抽屉等要上锁，钥匙要放在安全的地方，以保证他人即使在无人值守时也无法使用此计算机；此外，还应该禁止 DOS 或其他操作系统访问 NTFS 分区，在服务器上设置系统启动口令，设置 BIOS 禁用软盘引导系统，不创建任何 DOS 分区；保证机房的物理安全等。

2. 安装策略

采用自定义安装，设置系统文件格式为 NTFS，选择必要的系统组件和服务。因为协

议和服务安装得越多，入侵者入侵的途径越多，潜在的系统安全隐患也就越大。在 Windows NT 操作系统下，应该充分利用 NTFS 文件系统的安全性——NTFS 文件系统可以将每个用户允许读/写文件的权限限制在磁盘目录下的任何一个文件夹内。

3. 用户账户策略

（1）为用户设置密码策略

适当地使用密码策略并养成良好的习惯，可以将受到伤害的可能性降到最低，有效地避免攻击者获得受保护信息的访问权、在计算机中放入特洛伊木马或是进行其他的破坏活动。对于密码，我们可以创建密码策略来做些强制设置。

下面以使用“本地安全设置”控制台为例来设置安全策略。启动“本地安全设置”，打开“安全设置”→“账户策略”→“密码策略”，里面包含有密码必须符合复杂性要求、密码长度最小值、密码最长存留期、密码最短存留期、强制密码历史和为域中所有用户使用可以还原的加密来储存密码。例如，密码长度最小值就是指强制密码长度必须大于所设的数字，该数字最大值是 14。

（2）保护默认的管理员账户

管理员账户 Administrator 拥有整台计算机的完全控制权，任何人只要获得了管理员身份就可以在该台计算机上做他想做的任何事情。因为用户名是已知的，所以攻击者只需要破解密码就可以了。我们可以通过几个方面来保护默认的管理员账户：

- 为其指定一个保险的密码并且经常改变它。
- 修改 Administrator 账户的名称。
- 创建一个假的 Administrator 账户，将其指派到 Guests 组。

（3）设置用户锁定策略

账户锁定是指为保护账户的安全而将此账户进行锁定，使其在一定的时间内不能再次使用，以防止连续的尝试猜解口令攻击。账户锁定策略设定的第一步就是指定账户锁定的阈值，即锁定前该账户无效登录的次数 n。如果 n 次登录全部失败，就会锁定该账户。通过账户锁定策略，可以有效地避免自动猜解工具的攻击，同时对于手动尝试者的耐心和信心也可造成很大的打击。锁定用户账户常常会造成一些不便，但系统的安全有时更为重要。

使用“本地安全策略”控制台来设置用户锁定策略。方法如下：打开“本地安全设置”→“账户策略”→“账户锁定策略”。其中包括：账户锁定时间、账户锁定阈值、复位账户锁定计数器。账户锁定时间是指用户被锁定的时间，经过指定的时间之后，该用户会被自动解锁；账户锁定阈值是指在指定的时间内如果用户输入的错误密码次数达到了指定的数字，系统就会阻止该用户登录；复位账户锁定计数器是指在指定的时间内，如果用户输入密码错误达到了指定的次数，就会被锁定。

（4）限制用户登录

对于企业网的用户还可以通过对其登录行为进行限制，来保障其用户账户的安全。这样，即使是密码出现了泄漏，系统也可以在一定程度上将黑客拒之于门外。在 Windows NT 系统中，可以限制用户登录的时间和地点。其中，“登录时间”用来设置允许该用户登录的

时间，以防止非工作时间的登录行为；"登录到"用来设置允许该账户从哪些计算机上登录，限制非本机登录行为的发生。此外，还可以通过"账户"选项来限制登录时的行为。

4. 系统权限与安全配置

对系统设置，有一句话颇具代表性，即"最小的权限+最少的服务=最大的安全"。因此，在进行系统设置时，要始终设置用户所能允许的最小目录和文件的访问权限，还要关闭服务器上不必要的服务及端口。

（1）NTFS 系统权限设置

在使用之前，使每个硬盘的 Administrators 用户拥有全部权限（可选加入 system 用户）并删除其他用户，同时设置系统盘的权限如下：C:\Windows 目录下的 Administrators system 用户拥有全部权限，Users 用户默认权限不作修改；其他目录，删除 Everyone 用户。值得提醒的是，C:\Documents and Settings 下的 All Users 和 Default User 目录的默认配置是保留了 Everyone 用户权限的。C:\Windows 目录下面的权限也要注意，例如，C:\Windows\pchealth、C:\Windows\Installer 也是保留了 Everyone 权限的。

删除 C:\Windows\web\printers 目录，此目录的存在会造成 IIS 中加入一个.printers 的扩展名，可被用作溢出攻击。默认 IIS 错误页面已基本上很少有人使用了，建议删除 C:\Windows \Help\IISHelp 目录。删除 C:\Windows\system32\inetsrv\iisadmpwd，此目录通常用于管理 IIS 密码。

修改以下可执行文件的访问权限：net.exe、cmd.exe、tftp.exe、netstat.exe、regedit.exe、at.exe、attrib.exe、cacls.exe、format.com、regsvr32.exe、xcopy.exe、wscript.exe、cscript.exe、ftp.exe、telnet.exe、arp.exe、edlin.exe、 ping.exe、route.exe、finger.exe、posix.exe、rsh.exe、atsvc.exe、qbasic.exe、runonce.exe、syskey.exe。删除所有的用户，只保存 Administrators 组和 System 组为所有权限。

（2）删除默认共享、ipc$空连接，禁用不用端口

删除 Windows 的默认共享，可以提高系统的安全性。删除本地共享的步骤为：在"运行"对话框中输入"cmd"，按 Enter 键，在打开的命令行窗口中输入"net share admin$/delete net share c$/delete"，逐个删除。

删除 ipc$空连接的步骤为：在"运行"对话框中输入"regedit"，按 Enter 键，打开注册表编辑器，在注册表中找到 HKEY-LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 项里数值名称 RestrictAnonymous 的数值数据，由 0 改为 1。

为了进一步增加服务器系统的安全，应当把不用的端口一律关闭，只开放提供服务所必需的端口。配置的方法是设置 Internet 协议（TCP/IP）的属性，启用 TCP/IP 筛选，只允许开放服务器提供网络服务所必需的 TCP 端口。

139 端口是 NetBIOS 协议所使用的端口，在安装了 TCP/IP 协议的同时，NetBIOS 也会被作为默认设置安装到系统中。因为 139 端口具有 ipc 和 RPC 漏洞，它的开放意味着硬盘可能会在网络中共享，网上攻击者可能会利用这一漏洞掌握用户计算机的详细情况，所以需要将其关闭。具体方法是：网络和拨号连接→本地连接→Internet 协议（TCP/IP）属性→高级 TCP/IP 设置→WINS 设置，选择禁用 TCP/IP 的 NetBIOS，禁止 RPC 漏洞。

（3）服务最小化

在 Windows NT 上默认运行的服务有很多，但是大部分服务基本上是闲置不用的，却徒然增加了对系统的威胁。在 Windows Server 2003 中，有一些不必要的服务已被禁用（例如，DDE 服务等），但是仍然有一些不必要的危险服务（例如，Remote Registry 服务、SNMP 服务等）在运行，这些服务常常被攻击者利用。入侵者通过对目标服务器进行扫描，即可得到服务器上运行的服务类型等信息，进而找出服务器系统的安全漏洞。因此，对于那些没有实际意义的服务，应将其及时关闭。尤其是一些具有威胁性的服务，如 Computer Browse、Distributed File System、Messenger、Remote Registry、TCP/IP Net-BIOS Helper、Telnet 等，在安全性要求较高的服务器上，强烈建议将它们禁用。

5. 系统监控策略

尽管不断地在对系统进行修补，但由于软件系统的复杂性，新的安全漏洞总会层出不穷。

因此，除了对安全漏洞进行修补之外，还要对系统的运行状态进行实时监控，以便及时发现利用各种漏洞的入侵行为。

（1）启用系统审核机制。系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员进行分析、查找系统和应用程序故障以及各类安全事件。为了不影响系统性能，默认的安全策略并不对安全事件进行审核，对于关键的应用服务器和文件服务器来说，应启用所有的安全策略来发现黑客的入侵和入侵后的行为。

（2）日志监视。日志功能在某种程度上来说是入侵检测的得力帮手。在启用安全审核策略后，管理员应经常查看安全日志的记录，否则就失去了及时补救和防御的时机。除了安全日志外，管理员还要注意检查各种服务或应用的日志文件。应在本地安全策略中设置如下审核策略：账户管理操作成功及失败时记录事件；登录操作成功及失败时记录事件；对象访问操作失败时记录事件；策略更改操作成功及失败时记录事件；特权使用操作失败时记录事件；系统事件操作成功及失败时记录事件；目录服务访问操作失败时记录事件；账户登录操作成功及失败时记录事件。

（3）监视开放的端口和连接。对日志的监视只能发现已经发生的入侵事件，对于正在进行的入侵和破坏行为就无能为力了。这时，就需要管理员掌握一些基本的实时监视技术来应对。通常黑客或病毒入侵系统后，会在其中留下木马类后门；同时，它和外界的通信会建立一个 Socket 会话连接。此时利用 netstat 命令进行会话状态的检查，就可以查看已经打开的端口和已经建立的连接。当然，也可以采用一些专用的检测程序对端口和连接进行检测。

（4）监视共享。如果防范不严，最简单的入侵方法就是利用系统隐含的管理共享。因此，只要黑客能够扫描到 IP 和用户密码，就可以使用 net use 命令连接到共享上。另外，当浏览到含有恶意脚本的网页时，计算机的硬盘也可能被共享。因此，监测本机的共享连接是非常重要的。

6. 改进登录服务器

将系统的登录服务器移到一个单独的机器中，会提高系统的安全级别；使用一个更安全的登录服务器取代 Windows 自身的登录工具，也可以进一步增强安全性。在一个比较大的 Windows 网络中，最好建立一个域或者多个域，使用域服务器来统一管理系统登录。这个域服务器必须能够满足所有系统登录需求并且拥有足够的磁盘空间。在这个系统上，建议不要运行其他服务。使用域服务器管理用户，有利于削弱入侵者通过登录系统修改日志文件的能力。

7. 正确使用登录脚本

通过活动目录中的组策略制定系统策略和用户登录脚本，可以对网络用户的行为进行适当的限制。利用组策略编辑器为用户指定登录脚本，可以为用户设定工作环境，控制用户在桌面上进行的操作、执行的程序以及登录时间和地点等。

8. 应用系统的安全

在 Windows NT 上运行的应用系统，应及时通过各种途径获得补丁程序，以解决其安全问题；应将 IIS 中的 sample、scripts、iisadmin 和 msadc 等 Web 目录设置为禁止匿名访问并限制 IP 地址；将 FTP、Telnet 的 TCP 端口改为非标准端口；Web 目录、CGI 目录、scripts 目录和 WinNT 目录只允许管理员完全控制；凡是涉及到访问与系统有关的重要文件，除系统管理员账号 Administrator 外，其他账号均应设置为只读权限。

9. 及时备份

为了防止系统在使用的过程中发生意外情况而影响正常运行，应该对 Windows 完好的系统进行备份，最好是在完成 Windows 系统的安装任务后就对整个系统进行备份，以后可以根据这个备份来验证系统的完整性，这样就可以发现系统文件是否被非法修改过。

3.3.5 Windows NT 的数据保护

1. 使用 NTFS 文件系统保护数据

Windows NT 文件系统在 NTFS 分区上可以利用 NTFS 权限和文件加密提高数据安全性和数据存储有效性，利用数据压缩和磁盘配额提高磁盘空间的利用率。所以强烈建议在 Windows NT 系统中对磁盘格式化时，采用 NTFS 分区。

在 NTFS 分区上的每一个文件和文件夹都有一个列表，即访问控制列表 ACL。该列表记录了每一用户和组对该资源的访问权限。在 Windows NT 的 NTFS 权限下，用户必须获得明确的授权才能访问相应的文件和文件夹。NTFS 权限分为标准 NTFS 权限和特殊 NTFS 权限。

（1）标准 NTFS 权限

对于文件，标准 NTFS 权限分别为读取、写入、读取和运行、修改、完全控制。

① 读取：此权限可以读取文件内的数据，查看文件的属性、所有者、文件的权限等。

② 写入：此权限可以将文件覆盖、改变文件属性、查看文件的所有者、查看文件的权限等，但是不能直接更改文件内的数据。

③ 读取和运行：除了“读取”的所有权限外，还可以运行应用程序。

④ 修改：除了“读取”和“读取及运行”的所有权限外，还具有写入的权限，可以更改文件数据、删除文件、改变文件名等。

⑤ 完全控制：拥有所有 NTFS 权限，如可以修改权限、取得所有权等。

对于文件夹，标准 NTFS 权限分别为读取、写入、列出文件夹目录、读取和运行、修改、完全控制。

① 读取：此权限可以查看该文件夹内的文件和子文件夹名称，查看文件夹的属性、所有者、文件夹的权限等。

② 写入：此权限可以在文件夹内添加文件和文件夹、改变文件夹属性、查看文件夹的所有者、查看文件夹的权限等。

③ 列出文件夹目录：此权限除了拥有“读取”的所有权限外，还具有“遍历子文件夹”的权限，但不能在此文件夹下写入（不能创建新对象）。该权限只能被文件夹继承，而不能被文件继承。

④ 读取和运行：拥有读取的所有权限，同时可以运行文件夹下的可执行文件。和“列出文件夹目录”的权限一样，只是在权限的继承方面有所不同，“列出文件夹目录”权限只能由文件夹来继承，而“读取和运行”权限可由文件夹和文件同时继承。

⑤ 修改：除了“读取和运行”和“列出文件夹目录”的所有权限外，还具有写入的权限。可以添加和删除子文件夹、文件，改变子文件夹名等。

⑥ 完全控制：拥有所有 NTFS 权限，如可以修改权限、取得所有权等。

（2）特殊 NTFS 权限

特殊 NTFS 权限包含了在各种情况下对资源的访问权限，其规定约束了用户访问资源的所有行为。对于特殊的 NTFS 权限，只需了解其中两个使用比较频繁的权限——“更改权限”和“取得所有权”即可，其他的权限大多是组合标准 NTFS 权限在使用。

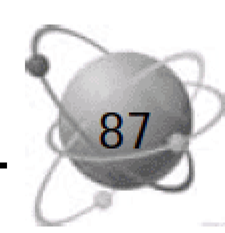
（3）NTFS 权限的继承性

NTFS 权限具有继承性，默认情况下，授予父文件夹的权限将被包含在该父文件夹下的子文件夹或文件所继承。也可以说，文件或文件夹默认继承分区或父文件夹的权限，并且继承来的权限不能直接设置和修改。

同一个 NTFS 分区内或不同 NTFS 分区之间移动或复制一个文件或文件夹时，该文件或文件夹的 NTFS 权限会发生不同的变化。在同一个 NTFS 分区内复制文件或文件夹时，复制文件和文件夹将继承目的位置中的文件夹的权限；在不同 NTFS 分区之间复制文件或文件夹时，复制文件和文件夹将继承目的位置中的文件夹的权限；在同一个 NTFS 分区内移动文件或文件夹时，文件和文件夹仍然保留在原位置的一切 NTFS 权限；在不同 NTFS 分区之间移动文件或文件夹时，文件和文件夹会继承目的分区中文件夹的权限。

（4）NTFS 权限的使用法则

一个用户可能属于多个组，而这些组又有可能被某种资源赋予了不同的访问权限，另



外的用户或组可能会对某个文件夹和该文件夹下的文件有不同的访问权限。在这种情况下，就必须通过 NTFS 权限法则来判断到底用户对资源有何种访问权限。

① 权限累加法则。当一个用户同时属于多个组，而这些组又有可能被某种资源赋予了不同的访问权限时，则用户对该资源的最终有效权限是在这些组中最宽松的权限，即累加权限，将所有的权限加在一起即为该用户的权限。

② 文件权限超越文件夹权限法则。当用户或组对某个文件夹以及该文件夹下的文件有不同的访问权限时，用户对文件的最终权限是用户被赋予访问该文件的权限，即文件权限超越其上级——文件夹的权限，用户访问该文件夹下的文件不受文件夹权限的限制，而只受被赋予文件权限的限制。

③ 拒绝权限超越所有其他权限法则。当用户对某个资源有拒绝权限时，该权限覆盖其他任何权限，即在访问该资源的时候只有拒绝权限是有效的。

2. 通过文件加密系统来提高数据安全性

EFS 加密系统只能在 NTFS 分区上实现，其加密是利用文件加密密钥来实现的。文件加密过程中将把文件加密密钥存储在文件头标中，与被加密的文件形成一个整体，因此当被加密的文件被移动到同一个磁盘分区的其他未加密文件夹中的时候，文件依然保持加密。EFS 用户如果是加密者本人，系统会在用户访问这些文件和文件夹时将其自动解密，用户完全不用参与。

在 Windows NT 中，每一个用户都有一个安全标识符（Security Identifier，SID），用以区分各自的身份。每个人的 SID 都是不相同的，即是有唯一性。可以这样理解：把 SID 想象成人的指纹，虽然世界上已经有几十亿人（同名同姓的也有很多），可是理论上还没有哪两个人的指纹是完全相同的。因此，这具有唯一性的 SID 就保证了 EFS 加密的绝对安全和可靠。因为理论上没有 SID 相同的用户，因而用户的密钥也就绝对不会相同。在第一次加密资料的时候，操作系统就会根据加密者的 SID 产生该用户的密钥，并把公钥和私钥分开存储起来，供用户加密和解密资料。

EFS 机制在设计时就考虑到了多种突发情况的产生，因此在 EFS 加密系统中，还有恢复代理这一概念。例如，公司财务部门的一个员工加密了财务报表，某天这位员工离职了。出于账户管理的目的，安全管理员通常会直接删除这位员工的账户。直到有一天要用到这位员工的财务报表时，才发现报表经过了加密，而用户账户已经删除，这些文件就无法打开了。恢复代理的存在，就是为了解决这个问题。因为被 EFS 加密过的文件，除了加密者本人之外还有恢复代理可以访问。对于 Windows 来说，在单机和工作组环境下，预设的恢复代理是 Administrator；而在域环境中，预设的恢复代理是域管理员。

制作备份密钥，可以避免因密钥丢失而无法访问文件的问题。在“运行”对话框中输入“certmgr.msc”，然后按 Enter 键，打开证书管理器。密钥的导入和导出的工作都将在这里进行。在当前用户→个人→证书路径下，可以看到一个以本用户名命名的证书（如果之前没有加密过任何资料，这里是不会有证书的）。右击这个证书，选择“导出”命令。之后会打开证书导出向导，通过此向导就可以导出用户的证书。导出的证书是一个以 pfx 为扩展名的文件。

在需要导入证书时，选择之前导出的以 pfx 为扩展名的文件，单击鼠标右键，选择“安装 PFX”命令，就可以打开证书导入向导。按照向导的提示完成操作，那么之前用该密钥加密过的资料就可以正常开启了。

3. 使用磁盘阵列来保护数据安全

系统容错技术可使计算机网络系统在发生故障时，保证系统仍能正常运行，继续完成预定的工作。Windows NT 网络系统的系统容错是建立在标准化的独立磁盘冗余阵列（RAID）基础上的，它采用软件解决方案，提供了 3 种 RAID 容错手段——RAID0、RAID1 和 RAID5。

（1）带区集（RAID0）

带区集是将多个磁盘上的可用空间组合成一个大的逻辑卷，数据将按系统规定的数据段为单位依次写入不同的磁盘上。虽然 RAID0 是顺序传送的，但多个读/写操作可以相互重叠进行，因此 RAID0 可提供较好的磁盘读写性能，但不提供任何容错功能。

（2）镜像集（RAID1）

镜像集由主磁盘和副磁盘两个磁盘组成。所有写入主磁盘的数据也同时写入副磁盘，如果主磁盘发生故障，则系统使用副磁盘中的数据。RAID1 通过两个磁盘互为备份，来提供数据保护。RAID1 主要用于提供存储数据的可靠性，但必须以较大的磁盘空间冗余为代价。

（3）带奇偶校验的带区集（RAID5）

在带奇偶校验的带区集中，阵列内所有磁盘的大块数据呈带状分布，数据和奇偶校验信息将存放在磁盘阵列中不同的磁盘上，以提高数据读写的可靠性。RAID5 具有较好的数据读取性能，但写入性能较差，通常需要消耗 3 倍读取操作的时间，因为写入操作时要进行奇偶校验计算。因此，RAID5 主要用于以读取操作为主的应用系统。

4. 数据的备份和还原

数据备份的目的就是为了成功地还原丢失和被破坏的数据。养成良好的数据备份习惯是一名合格的网络工程师应该具备的基本素质。Windows NT 中提供了一个专门的工具——“备份”来完成数据的备份和还原工作。不过备份和还原数据并非人人适用，用户必须拥有相应的系统权限才可以。

用户可以备份自己的文件和文件夹，也可以备份具有“读取”权限的文件和文件夹。所有用户都可以还原具有“写入”权限的文件和文件夹；Administrators 组、Backup Operators 组和 Server Operators 组的成员可以备份和还原所有文件和文件夹。

通常的备份操作可能会由普通用户来完成，因此出于安全性的考虑，需要将这些用户加入到 Backup Operators 组中而不是将其加入到 Administrators 组或 Server Operators 组中，因为这些组具有更多其他的权限。

（1）数据备份的类型

在介绍备份类型之前有一个概念需要知道，这就是文件的“存档”属性。文件的“存档”属性对于数据备份有着非常重要的意义。在备份一个文件时，为了提高效率和节省时

间，应当只备份改动过的数据，对于没有改动的数据不进行备份，这样的效率是最高的，而所花费时间是最少的。文件的“存档”属性恰好可以达到这个目的。因为任何一个新建的文件，系统都会自动为其添加一个“存档”属性，当使用备份程序备份这个文件之后，系统会自动将“存档”属性清除以表示该文件已经被备份过了。当该文件被改动之后，系统又会自动为其添加上“存档”属性，在下一次备份时，备份程序就会备份该文件。如果某种备份类型不清除“存档”属性，则在下次备份时还要备份该数据。

在 Windows Server 2003 中备份程序提供了 5 种备份类型：正常、副本、差异、增量和日备份。下面具体介绍这 5 种备份类型的特点。

① 正常（Normal）：提供最完整的备份，将所有选定的文件和文件夹进行备份。该备份花费的时间是最长的，但在恢复时是最容易的。

② 副本（Copy）：备份所有选择的文件和文件夹，但是不清除文件的“存档”属性。

③ 差异（Differential）：在选定的文件和文件夹中，只备份从上次备份之后发生改动过的数据且不清除文件的“存档”属性。

④ 增量（Increamental）：在选定的文件和文件夹中，只备份从上次备份之后发生改动过的数据，但是在备份操作完成之后会清除“存档”属性。

⑤ 日备份（Daily）：只备份当天有过改动的文件，即使是几天前更改过的文件有“存档”属性也不备份。该备份类型不清除“存档”属性。

（2）数据还原

数据还原就是当系统出现故障而丢失数据时将数据恢复到原来的状态，这是一个备份的逆向过程。

3.4 UNIX/Linux 操作系统安全

在安全结构上，Linux 与 UNIX 基本上是相似的，它们都具有以下安全特征。

1. 访问控制

系统通过访问控制表 ACL，使用户可以自行改变文件的安全级别和访问权限。系统管理员可用 umask 命令为每个用户设置默认的权限值，用户也可以通过 chmod 命令来修改自己拥有的文件或目录权限。

2. 对象的可用性

当一个对象不再使用时，在它回到自由对象之前，系统将会清除它，以备下次需要时使用。

3. 身份标识与认证

UNIX/Linux 系统为了确定用户的真实身份，在用户登录时采用扩展的 DES 算法对输入的口令进行加密，然后把口令的密文与存放在/etc/passwd 中的数据进行比较，如果二者的值完全相同，则允许用户登录到系统中，否则将禁止用户的登录。

4. 审计记录

UNIX/Linux 系统能够对很多事件进行记录，例如文件的创建和修改以及系统管理的所有操作和其他有关的安全事件（例如，登录失败，以 root 身份进行登录的情况等）。通过这些记录，系统管理员就可以对安全问题进行跟踪。

5. 操作的可靠性

操作的可靠性是指 UNIX/Linux 系统用于保证系统完整性的能力。UNIX/Linux 系统通过对用户的分级管理、运行级别的划分，以及访问控制机制加上自带的一些工具，能够很好地保证系统操作的可靠性。

3.4.1 超级用户安全管理

root 用户在 UNIX/Linux 系统中具有无限的权力，可以进行任何操作。root 用户可以进行如下具有潜在危险的操作：

（1）添加、删除或者更改所有其他用户的账户。

（2）读写所有文件，以及创建新文件。

（3）添加/删除系统中的设备。

（4）安装新的系统软件。

（5）读取任何人的电子邮件。

（6）在局域网中探测网络通信，获取其他系统的用户名和密码。

（7）更改系统中所有的日志，删除所有超级用户访问的记录。

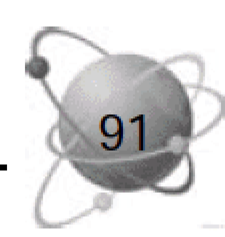
（8）冒充非特权用户，访问他们在其他需要验证登录访问的系统中的账户。

这些权力混合起来，使得 root 账户听起来很危险。不过，这其中许多操作是合理合法的，并且是每天必要的系统管理例行工作。例如，探测网络通信情况可以确定在什么地方产生了网络拥塞。不过，如果一个入侵者获取到 root 权限，情况就大不妙了。他可以在系统中为所欲为，如删除或者窃取数据，删除或添加用户账户，或者安装特洛伊木马，从而透明地更改系统工作的方式。使用 su 命令获取了 root 权限，root 用户就可以使用 su 命令变为系统中任何其他用户，并启动具有有效 ID 的 Shell。这是一个安全漏洞：root 用户可以冒充其他用户对数据进行操作和更改；对这些操作进行跟踪，最终只能跟踪到有效用户，而不是 root。

一种比较有效的防止授权用户获取 root 权限的方法，是使用一个难以猜测的 root 密码。最佳的密码是完全随机的字母、数字和标点符号组合而成的字符串。不要写下 root 用户的密码，也不要把密码告诉其他的用户。

3.4.2 用户账户安全管理

每个账户都是具有不同用户名、不同口令和不同访问权限的一个单独实体，用户也就



有权授予或拒绝任何用户、用户组和所有用户的访问。用户可以生成自己的文件，安装自己的程序等。为了确保次序，系统会分配好用户目录，每个用户都会得到一个主目录和一块硬盘空间，并与其他用户占用的区域分割开来。这种做法可以防止一般用户的活动影响其他文件系统，进而系统还为每个用户提供一定程度的保密。作为根可以控制哪些用户能够进行访问以及他们可以将文件存放的位置，控制用户能够访问哪些资源以及如何进行访问等。用户登录到系统中时，需输入用户名标识其身份。当该用户的账户创建时，系统管理员便为其分配一个唯一的标识号——UID。系统中的/etc/Passwd 文件含有全部系统需要知道的关于每个用户的信息（加密后的口令也可能存于/etc/shadow 文件中）。/etc/Passwd 中包含有用户的登录名、经过加密的口令、用户号、用户组号、用户注释、用户主目录和用户所用的 Shell 程序。其中用户号 UID 和用户组号 GID 用于 UNIX 系统唯一地标识用户和同组用户及用户的访问权限。系统中，超级用户 root 的 UID 为 0。每个用户可以属于一个或多个用户组，每个组由 GID 唯一标识。

在大型的分布式系统中，为了统一对用户进行管理，通常将每一台工作站上的口令文件信息存在网络服务器上。目前流行的系统有：SUM 公司的网络信息系统 NIS；Sun 公司的 NIS+；开放软件基金会的分布式计算机环境 DCE。

3.4.3　用户口令安全管理

用户名是个标识，用于告诉计算机该用户是谁；而口令是个确认证据，用户登录系统时，便需要输入口令来鉴别用户身份。当用户输入口令时，UNIX/Linux 使用改进的 DES 算法（通过调用 eryPt()函数实现）对其进行加密，并将结果与存储在/etc/passwd 或 NIS 数据库中的加密用户口令进行比较。若二者匹配，则说明该用户的登录合法；否则拒绝用户登录。为防止口令被非授权用户盗用，对其设置应以复杂、不可猜测为标准。一个好的口令应当至少有 8 个字符长度。不要取用个人信息，普通的英语单词也不好（因为可用字典攻击法）。口令中最好有一些非字母（例如，数字、标点符号、控制字符等）。用户应定期改变口令。通常口令以加密的形式表示。由于/etc/passwd 文件对任何用户可读，故常成为口令攻击的目标。所以系统中常用 shadow 文件（/etcjshadow）来存储加密口令，并使其对普通用户不可读。

3.4.4　文件和目录的安全

UNIX/Linux 文件系统可控制文件和目录中的信息以何种方式存储在磁盘及其他辅助存储介质上、每个用户可以访问何种信息及如何访问。其具体表现形式为一组存取控制规则，可以据此确定一个主体是否可以存取一个指定客体。UNIX/Linux 的存取控制机制通过文件系统实现。

文件的权限是 UNIX/Linux 系统安全的第一道防线。UNIX/Linux 权限的基本类型有读、写和执行，每种权限的具体解释如表 3-2 所示。

表 3-2 UNIX/Linux 基本权限的解释

权　限	应用于目录	应用于任何其他类型的文件
读（r）	授予读取目录或子目录内容的权限	授予查看文件的权限
写（w）	授予创建、修改或删除文件或子目录的权限	授予写入的权限，允许一个经过授权的实体修改文件
执行（x）	授予进入目录的权限	允许用户运行程序
-	无权限	无权限

每个文件的权限都是用左起第 2～10 个字符来记录，第 1 个字符表示文件类型。权限分成 3 组，每组有 3 个字符，组中的每个位置对应一个指定的权限，其顺序为读、写、执行。前 3 个字符（2～4）表示文件所有者的权限（本例中是 student）；第 2 组的 3 个字符（5～7）表示文件所属组的权限（示例中为 staff）；最后一组的 3 个字符（8～10）表示其他任何人的权限。

下面是 ls-l 命令的输出示例，其中包括一个文件和一个目录。

```
$ls-1/home/student
-rwxr-xr--   1   student   staff   1024   oct  2  00:10  testfile
Drwxr-xr--   1   student   staff   1024   oct  2  00:10  testdir
```

根据前面所讲的原则，在该例中 testfile 的权限为：文件的所有者（student）对文件具有读取、写入和执行的权限；该文件所属的组（staff）中的用户可以读取和执行该文件，没有对文件写入的权限；有效登录到系统的其他用户只能读取该文件。

要修改文件或目录权限，可以使用 chmod（change mode）命令。文件权限的第一个集合（1s-l 命令输出的第 2～4 个字符）用字母 u 来表示，代表用户；第二个集合（字符 5～7）用 g 来表示，代表组；最后一个集合（字符 8～10）用 o 来表示，代表其他任何人（其他）。此外，还可以使用-a 选项同时对所有 3 个组进行授权或者删除其权限。

借助于表 3-3 中的操作符，可以利用符号权限来添加、删除或指定权限集合。示例文件 testfile1 的原始权限为 rwxrwxr--。

表 3-3 Chmod 操作符

Chmod 操作符	含　义	示　例	结　果
+	为一个文件或目录添加指定的权限	Chmod o+x testfile1	为 testfile1 文件的其他用户添加执行权限
–	从一个文件或目录中删除指定的权限	Chmod u-x testfile1	删除文件所有者执行 testfile1 的权限
=	设置指定的权限	Chmod g=r-- testfile1	为组设置 testfile1 的读取权限，不能写入和执行

3.4.5 关于 SUID 程序

有时没有被授权的用户需要完成某些要求授权的任务，例如 passwd 程序。对于普通用

户，系统允许他改变自身的口令，但不能拥有直接访问/etc/passwd 文件的权限，以防止他改变其他用户的口令。为了解决这个问题，UNIX 允许对可执行的目标文件（只有可执行文件才有意义）设置 SUID（Set User ID）或 SGID（Set Group ID）。

当一个进程在执行时，就被赋予 4 个编号（分别为实际和有效的 UID、实际和有效的 GID），以标识该进程隶属于谁。有效的 UID 和 GID 一般和实际的 UID 和 GID 相同，用于系统确定该进程对于文件的存取许可。而设置可执行文件的 SUID 许可，将改变上述情况。当设置了 SUID 时，进程的有效 UID 为该可执行文件的所有者的有效 UID 而不是执行该程序的用户的有效 UID。因此，执行该程序的用户拥有与该程序所有者相同的存取许可。这样，程序的所有者即可通过程序的权限控制，在有限的范围内向用户发表不允许被公众访问的信息。同样，SGID 也是设置有效 GID。用“chmod u+s 文件名”和“chmod u-s 文件名”来设置和取消 SUID 设置；用“chmod g+s 文件名”和“chmod g-s”文件名来设置和取消 SGID 设置。

小　结

网络操作系统 NOS 是向网络计算机提供网络通信和网络资源共享功能的操作系统。它是负责管理整个网络资源和方便网络用户的软件集合，是整个网络的灵魂。

操作系统安全是指该系统能够控制外部对系统信息的访问，即只有经过授权的用户或进程才能对信息资源进行相应的读、写、创建和删除等操作，以保护合法用户对授权资源的正常使用，防止非法入侵者对系统资源的侵占和破坏。

访问控制是操作系统中最有效、最直接的安全措施，是操作系统安全机制的关键。访问控制是在身份认证的基础上，根据用户身份对提出的资源访问请求加以控制，是针对越权使用资源的现象进行防御的措施。访问控制按照其不同的实现方法，可以分为自主访问控制、强制访问控制、基于角色的访问控制、基于任务的访问控制和基于对象的访问控制等。

具体的访问控制措施有：入网访问控制、资源访问控制、网络服务器安全控制、网络端口和节点的安全控制、网络监测、锁定控制以及防火墙控制。

Windows NT 是 Microsoft 推出的面向工作站、网络服务器和大型计算机的网络操作系统，也可用作 PC 机操作系统。Windows NT 提供了两个微软管理界面 MMC 的插件作为安全性配置工具，即安全性模板和安全性配置分析。安全性模板提供了针对 10 多种角色（从基本工作站、基本服务器一直到高度安全性的域控制器）的计算机管理模板。

Windows NT 采用的安全技术有活动目录和域、Kerberos 验证协议、加密文件系统 EFS 和 Windows IP Security 安全性支持等。

Windows NT 的安全管理措施包括物理安全、安装策略、用户账户策略、系统权限与安全配置、系统监控策略、改进登录服务器、正确使用登录脚本、应用系统的安全和及时备份。

Windows NT 的数据保护方法有使用 NTFS 文件系统保护数据、通过文件加密系统来提高数据安全性、使用磁盘阵列来保护数据安全、数据的备份和还原。

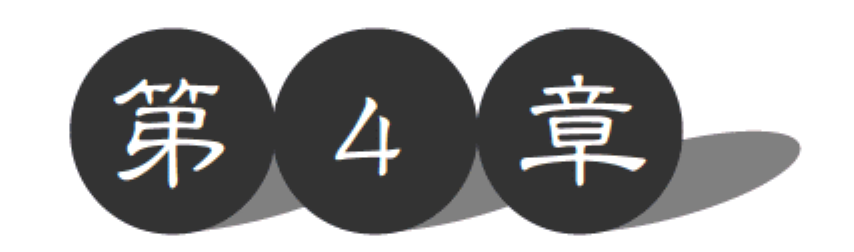
在安全结构上，Linux 与 UNIX 基本上是相似的，它们都具有访问控制、对象的可用性、身份标识与认证、审计记录和操作的可靠性等安全特征。

root 用户在 UNIX/Linux 系统中具有无限的权力，可以进行任何操作。防止授权用户获取 root 权限的一种方法是使用一个难以猜测的 root 密码。最佳的密码是完全随机的字母、数字和标点符号组合而成的字符串。不要写下 root 用户的密码，也不要把密码告诉其他用户。

由于每个账户都是具有不同用户名、不同口令和不同访问权限的一个单独实体，用户也就有权授予或拒绝任何用户、用户组和所有用户的访问。当用户输入口令时，UNIX/Linux 使用改进的 DES 算法对其加密。UNIX/Linux 文件系统控制文件和目录中的信息以何种方式存储在磁盘及其他辅助存储介质上，并控制每个用户可以访问何种信息及如何访问。

练习与思考

1. 什么是网络操作系统？
2. 常见的网络操作系统有哪几种？
3. 操作系统安全的含义是什么？
4. 什么是基于角色的访问控制？
5. 什么是基于任务的访问控制？
6. 什么是基于对象的访问控制？
7. Windows NT 系统采用了哪些安全技术？
8. 查阅资料，根据实际应用设计 Windows Server 2003 系统的安全配置方案。
9. 在 NTFS 文件系统中，文件访问权限的使用法则是什么？
10. Windows Server 2003 的 5 种数据备份类型及其特点是什么？
11. UNIX/Linux 操作系统的安全特征是什么？
12. 解释-rwxr-rw-的含义。
13. UNIX/Linux 操作系统账户的安全管理应该注意哪些问题？



第4章 数据库与数据安全

本章学习要求：

（1）掌握数据库系统的安全性要求、故障类型、基本安全架构和安全特性。
（2）掌握数据库的各种安全机制和数据库安全的保护措施。
（3）掌握数据库的备份与恢复方法。
（4）掌握 SQL Server 数据库的安全保护方法、策略。
（5）了解攻击数据库的常用方法。
（6）了解 Web 数据库的安全。

重点和难点：

（1）重点：掌握数据库系统的安全性要求、故障类型、基本安全架构和安全特性。
（2）难点：掌握数据库的各种安全机制和数据库安全的保护措施。

随着数据信息计算机网络化的飞速发展，数据库在各个领域都得到了广泛的应用，越来越多的部门和机构依赖于计算机网络传输、存储数据信息，但随之而来数据的安全问题变得日益突出。各种系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，关系到企业兴衰、国家安全。因此，如何有效地保证数据库系统的安全，实现数据存储或传输的保密性、完整性和有效性，已经成为业界人士探索研究的重要课题之一。

4.1 数据库安全概述

20 世纪 70 年代初，美国军方率先发起对多级安全数据库管理系统（Multilevel Secure Database Management System，MLS DBMS）的研究，此后一系列数据库安全模型被提出。

20 世纪 80 年代，美国国防部根据军用计算机系统的安全需要，制定了《可信计算机

系统安全评估标准》(Trusted Computer System Evaluation Criteria，TCSEC)，以及该标准的可信数据库系统的解释（Trusted Database Interpretation，TDI)，从而形成了最早的信息安全及数据库安全评估体系。TCSEC/TDI 将系统安全性分为 4 组 7 个等级，依次是 D（最小保护)、C1（自主安全保护)、C2（受控存取保护)、B1（标记安全保护)、B2（结构化保护)、B3（安全域）和 A（验证设计)，按系统可靠或可信程度逐渐增高。

20 世纪 90 年代后期，《信息技术安全评价通用准则》(Common Criteria，CC）被 ISO 接受为国际标准，确立了现代信息安全标准的框架，为安全数据库系统的研究及其应用系统的开发提供了指引。

在安全数据库需求及信息安全标准的推动下，国外各大主流数据库厂商相继推出了各自的安全数据库产品，例如 Sybase 公司的 Secure SQL Server、Oracle 公司的 Trusted Oracle 7 和 Informix 公司的 Informix-online/Secure 5.0 等。近几年来，Oracle 公司的 Oracle 9i 和 Oracle 10g 从用户认证、访问控制、加密存储和审计策略等方面进一步加强了安全控制功能。

我国从 20 世纪 80 年代开始着手进行数据库技术的研究和开发，而安全数据库理论的研究和实际系统的研制也于 90 年代初陆续展开。2001 年，我国军方提出了第一个数据库安全标准——《军用数据库安全评估准则》。2002 年，公安部发布了公安部行业标准——《计算机信息系统安全等级保护/数据库管理系统技术要求》(GA/T 389—2002)。

20 世纪 90 年代以来，华中科技大学、中国人民大学和东北大学等单位纷纷对数据库安全技术研究和实践，并相继开发出了相应的安全数据库软件，例如基本达到 B1 级安全要求的 DM3 数据库、COBASE（KingBase）数据库 2.0 可信版本及 OpenBase Secure 等。2003 年，中科院信息安全国家重点实验室基于开放源代码的数据库管理系统 Postgre SQL 开发出安全数据库系统 LOIS。

总体来说，与国外主流数据库产品相比，我国的研究成果在安全性和可用性上还有一定的差距。根据 2004 年底的统计，几大国外数据库管理系统在国内的市场占有率达到 95%，而国产数据库仅占到大约 3.5%，其他开发的产品大约占 1.5%。国外的数据库产品不提供源程序代码，也很少有可供公开调用的内核接口，从而加大了自主安全保护的技术难度；加之发达国家限制 C2 级以上安全级别的信息技术与产品对我国的出口，所以研究开发拥有自主知识产权的数据库安全控制技术具有非常重要的现实意义，任重而道远。

4.1.1 数据库安全的概念

数据库安全是指为存放数据的数据库系统制定、实施相应的安全保护措施，以保护数据库中的数据不因偶然或恶意的原因而遭到破坏、更改和泄露。目前，数据库安全与网络安全、操作系统安全及协议安全一起构成了信息系统安全的 4 个最主要的研究领域。数据库安全主要包括系统运行安全和系统信息安全两层含义。

1. 系统运行安全

系统运行安全包括：法律、政策的保护，例如用户是否有合法权限、政策是否允许等；

物理控制安全，例如机房是否加锁等；硬件运行安全；操作系统安全，例如数据文件是否受保护等；灾害、故障恢复；死锁的避免和解除；防止电磁信息泄漏。

2. 系统信息安全

系统信息安全包括：用户口令鉴别；用户存取权限控制；数据存取方式控制；审计跟踪；数据加密。

4.1.2 数据库管理系统及其特性

数据、数据库、数据库管理系统和数据库系统是与数据库技术密切相关的 4 个基本概念。

1. 数据库系统简介

（1）数据库系统的组成：数据库系统分成两部分，一部分是数据库，按一定的方式存取数据；另一部分是数据库管理系统，为用户及应用程序提供数据访问，并具有对数据库进行管理、维护等多种功能。

（2）数据库：若干数据的集合体。数据库要由数据库管理系统进行科学的组织和管理，以确保数据库的安全性和完整性。

（3）数据库管理系统：对数据库进行管理的软件系统，为用户或应用程序提供了访问数据库中的数据和对数据的安全性、完整性、保密性、并发性等进行统一控制的方法。

（4）数据库系统：以数据库方式管理大量共享数据的计算机系统，一般简称为数据库。数据库系统是由外模式、模式和内模式组成的多级系统结构。作为管理大量的、持久的、可靠的、共享的数据工具，数据库系统通常由数据库、数据库管理系统、硬件和软件支持系统以及用户 4 个部分构成。

2. 数据库管理系统的功能

数据库管理系统（DBMS）的基本功能是定义数据库，进行数据的存取，实现基本的数据管理和维护等功能。

（1）数据库定义：定义外模式、模式、内模式、数据库完整性、安全保密、存取路径等。

（2）数据存取：提供数据的操纵语言，以便对数据进行查找和更新。

（3）数据库运行管理：事务管理、自动恢复、并发控制、死锁检测或防止、安全性检查、存取控制、完整性检查、日志记录等。

（4）数据组织、存储和管理：数据字典、用户数据、存取路径的组织存储和管理，以便提高存储空间利用率，并方便存取。

（5）数据库的建立和维护：数据转换、数据库新建、转储、恢复、重组、重构以及性能检测等。

（6）网络通信、数据转换、异构数据库互访等。

3. 数据库管理系统的特性

（1）数据的安全性

数据的安全主要是保证数据存储处的安全和数据在访问或传输过程中不被窃取或恶意破坏，因此需要对数据进行一些安全控制，如将数据加密，以密码的形式存于数据库内，并将数据库中需要保护的部分与其他部分隔离；使用授权规则鉴别用户身份，阻止非法主体的访问等。

（2）数据的结构化

在文件系统中，文件内部的数据一般是有结构的，但文件之间不存在联系，因此从数据的整体来说是没有结构的。数据库系统虽然也常常分成许多单独的文件，并且文件内部也具有完整的数据结构，但是它更注重同一数据库中各文件之间的相互联系，故特别能适应大量数据管理的客观需要。

（3）数据共享

共享是数据库系统的目的，也是其重要特点。一个数据库中的数据，不仅可以为同一企业或组织内部的各部门共享，还可以为不同组织、地区甚至不同国家的用户所共享。

（4）数据独立性

在文件系统中，数据结构和应用程序是相互依赖的，任何一方的改变总是要影响另一方的改变。在数据库系统中，这种相互依赖性是很小的，数据和程序具有相对的独立性。

（5）可控冗余度

在文件系统中，由于每个应用都拥有并使用自己的数据，各文件中难免有许多数据相互重复，产生了冗余。数据库系统是面对整个系统的数据共享而建立的，各个应用的数据集中存储、共同使用，因而尽可能地避免了数据的重复存储，减少了数据的冗余。

4.1.3 数据库管理系统的缺陷和威胁

随着计算机技术的飞速发展，数据库在各个领域都得到广泛的应用，在为人们的工作、学习带来便利的同时，其安全问题也变得日益突出。数据库中存储的信息越来越有价值，一旦这些信息暴露，其后果不堪设想。因此，各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。

1. 数据库管理系统的缺陷

目前市场上流行的关系型数据库管理系统的安全性较差，从而导致数据库系统的安全性存在一定的威胁。常见数据库的安全漏洞和缺陷有：

（1）数据库应用程序通常都同操作系统的最高管理员密切相关。

（2）人们对数据库安全的忽视。

（3）部分数据库机制威胁网络低层安全。

（4）安全特性缺陷。

（5）数据库账号、密码容易泄漏。

（6）操作系统后门。

（7）木马的威胁。

2．数据库管理系统受到的威胁

发现威胁数据库安全的因素和采取相应的措施是解决数据库安全问题的两个方面，二者缺一不可。数据库管理系统的威胁主要有篡改、损坏和窃取等。

（1）篡改

篡改是指对数据库中的数据未经授权地进行修改，使其失去原来的真实性。篡改是一种人为的主动攻击，进行这种人为攻击的原因可能是个人利益驱动、隐藏证据、恶作剧或无知。

（2）损坏

损坏的表现为数据库中的数据表和整个数据库部分或全部被删除、移走或破坏。产生损坏的原因主要有人为破坏、恶作剧和病毒。

（3）窃取

窃取一般只针对敏感数据，被窃取的数据可能具有很高的价值，窃取的手法可能是将数据复制到可移动的介质上带走或把数据打印后取走，窃取数据的对象一般是内部员工和军事及工商业间谍等。

3．数据库系统威胁的来源

数据库安全的威胁主要来自以下几个方面：

（1）物理和环境的因素。

（2）事务内部故障。

（3）系统故障。

（4）人为破坏。

（5）介质故障。

（6）并发事件。

（7）病毒与黑客。

4.2　数据库的安全特性

从本质上讲，数据库安全依赖于数据库系统的访问控制（一是控制物理访问，二是通过 DBMS 控制访问）。所有 DBMS 都包含安全保护系统，数据库保护主要包括数据独立性、数据安全性、数据的完整性、并发控制和故障恢复。

4.2.1　数据库的安全特性

1．数据库的安全性

数据库的安全性从字面上理解含义很广，诸如防火、防盗、防震、防掉电等，这些措

施对于数据库的安全固然重要，但本章所讨论的安全性是指在数据库管理系统的控制之下保护数据，以防止不合法的使用而造成的数据泄漏、更改和破坏。

引发数据库安全性问题的因素主要有以下几种：

（1）政策问题。例如，拥有系统的企业内部确定数据存取原则，只允许指定用户存取指定数据。

（2）法律、社会和伦理问题。例如，请求者是否拥有对所请求信息的合法权限。

（3）硬件控制。例如，CPU 是否具备安全性方面的特性。

（4）物理控制。例如，计算机或终端所在房间是否上锁或受到保护。

（5）操作系统支持。例如，底层操作系统在退出后是否抹去了主存储器和磁盘上文件的内容。

（6）可操作性问题。若某个密码方案被采用，则密码自身的安全性如何保证。

（7）数据库系统本身的安全性问题。

2. 数据库的安全机制

数据库的安全机制是用于实现数据库的各种安全策略的功能集合，正是由这些安全机制来实现安全模型，进而实现保护数据库系统安全的目标。近年来，对用户的认证与鉴别、存取控制、数据库加密及推理控制等安全机制的研究取得了不少新的进展。

（1）用户标识与鉴别

数据库系统不允许一个未经授权的用户对数据库进行操作。用户标识和鉴别是系统提供的最外层的安全保护措施。在数据库管理系统中注册时，每个用户都有一个用户标识符。但一般来说，用户标识符仅是用户公开的标识，尚不足以成为鉴别用户身份的凭证。为了鉴别用户身份，一般采用以下几种方法：

① 利用只有用户知道的信息鉴别用户。

② 利用只有用户具有的物品鉴别用户。

③ 利用用户的个人特征鉴别用户。

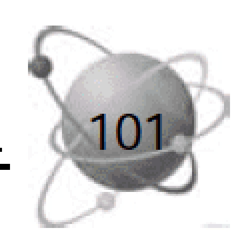
（2）存取控制

存取控制是对用户的身份进行识别和鉴别，对用户利用资源的权限和范围进行核查，是数据保护的前沿屏障。它可以分为身份认证、存取权限控制、数据库存取控制等几个层次。

① 身份认证。身份认证的目的是确定系统和网络的访问者是否是合法用户。主要采用密码、代表用户身份的物品（例如磁卡、IC 卡等）或反映用户生理特征的标识（例如指纹、手掌纹理、语音、视网膜扫描等）鉴别访问者的身份。

② 存取权限控制。存取权限控制的目的是防止合法用户越权访问系统和网络资源，即确定用户对哪些资源（例如 CPU、内存、I/O 设备程序、文件等）享有使用权以及可进行何种类型的访问操作（例如读、写、运行等）。为此，系统要赋予用户不同的权限，例如普通用户或有特殊授权的计算机终端或工作站用户、超级用户、系统管理员等，用户的权限等级是在注册时赋予的。

③ 数据库存取控制。对数据库信息按存取属性划分的授权有：允许或禁止运行，允许



或禁止阅读、检索，允许或禁止写入，允许或禁止修改，允许或禁止清除等。

3. 授权和角色

（1）授权

DBMS 提供了功能强大的授权机制，可以给用户授予各种不同对象（表、视图、存储过程等）的不同使用权限（例如 Select、update、insert、delete 等）。

用户级别可以授予的数据库模式和数据操纵方面的权限有：创建和删除索引、创建新关系、添加或删除关系中的属性、删除关系、查询数据、插入新数据、修改数据、删除数据等。

在数据库对象级别上，可将上述访问权限应用于数据库、基本表、视图和列等。

（2）角色

如果要给成千上万个雇员分配许可，将面临很大的管理难题，如每次有雇员到来或者离开时，就得有人分配或去除可能与数百张表或视图有关的权限，劳心费力不说，还容易出错。一个相对简单有效的解决方法就是定义数据库角色。数据库角色是被命名的一组与数据库操作相关的权限，即一组相关权限的集合。可以为一组具有相同权限的用户创建一个角色。使用角色来管理数据库权限，可以简化授权的过程。

4. 视图机制

几乎所有的 DBMS 都提供视图机制。视图不同于基本表，它不存储实际数据。当用户通过视图访问数据时，是从基本表中获得数据。视图提供了一种灵活而简单的方法，以个人化方式授予访问权限，能够起到很好的安全保护作用。在授予用户对特定视图的访问权限时，该权限只用于在该视图中定义的数据项，而不是用于视图对应的完整基本表。

5. 审计

对数据库管理员（DBA）而言，审计就是记录数据库中正在做什么的过程。审计记录可以告诉 DBA 某个用户正在使用哪些系统权限，使用频率是多少，多少用户正在登录，会话平均持续多长时间，正在特殊表上使用哪些命令，以及其他有关事实。

审计一般可以分为用户级审计和系统级审计两级。任何用户均可设置用户级审计，主要是针对自己创建的数据库或视图进行审计，记录所有用户对这些表或视图的一切成功和不成功的访问要求，以及各种类型的 SQL 操作；系统级审计只能由 DBA 设置，用以监测成功或失败的登录请求、监测 Grant 和 Revoke 操作以及其他数据库级权限下的操作。

通过审计功能可将用户对数据库的所有操作自动记录下来，放入审计日志（Audit Log）中。审计日志一般包括下列内容：

（1）操作类型（例如修改、查询等）。

（2）操作终端标识与操作人员标识。

（3）操作日期和时间。

（4）操作的数据对象（例如表、视图、记录、属性等）。

（5）数据修改前后的值。

4.2.2 数据库的完整性

数据库完整性是指数据库中数据的正确性和兼容性。数据库完整性由各种各样的完整性约束来保证，因此可以说数据库的完整性设计就是数据库完整性约束的设计。

数据库的完整性主要包括物理完整性和逻辑完整性。物理完整性是指保证数据库中的数据不受物理故障（例如硬件故障或掉电等）的影响，并有可能在灾难性毁坏时重建和恢复数据库；逻辑完整性是指对数据库逻辑结构的保护，包括数据语义与操作完整性。前者主要指数据存取在逻辑上满足完整性约束；后者主要指在并发事务中保证数据的逻辑一致性。

数据库完整性约束可以通过 DBMS 或应用程序来实现，基于 DBMS 的完整性约束作为模式的一部分存入数据库中。通过 DBMS 实现的数据库完整性按照数据库设计步骤进行设计，而由应用软件实现的数据库完整性则纳入应用软件设计。

数据库完整性对于数据库应用系统非常关键，其作用主要体现在以下几个方面。

（1）数据库完整性约束能够防止合法用户使用数据库时向数据库中添加不合语义的数据。

（2）利用基于 DBMS 的完整性控制机制来实现业务规则，易于定义，容易理解，而且可以降低应用程序的复杂性，提高应用程序的运行效率。同时，基于 DBMS 的完整性控制机制是集中管理的，因此比应用程序更容易实现数据库的完整性。

（3）合理的数据库完整性设计，能够同时兼顾数据库的完整性和系统的效能。例如，装载大量数据时，只要在装载之前临时使基于 DBMS 的数据库完整性约束失效，此后再使其生效，就既能保证不影响数据装载的效率又能保证数据库的完整性。

（4）在应用软件的功能测试中，完善的数据库完整性有助于尽早发现应用软件的错误。

数据库完整性约束可分为 6 类：列级静态约束、元组级静态约束、关系级静态约束、列级动态约束、元组级动态约束、关系级动态约束。动态约束通常由应用软件来实现。不同 DBMS 支持的数据库完整性基本相同。

4.2.3 数据库的并发控制

1. 数据库并发控制的含义

数据库系统一般可分为单用户系统和多用户系统两种。在任一时刻只允许一个用户使用的数据库系统称为单用户数据库系统，允许多个用户同时使用的数据库系统称为多用户数据库系统。数据库的最大特点之一就是数据资源共享，因而多数数据库系统都是多用户系统，这样就会发生多个用户并发存取同一数据块的情况，如果对并发操作不加以控制就可能产生不正确的数据，破坏数据库的完整性。并发控制就是为了解决这类问题，以保持数据库中数据的一致性。

2. 事务

事务（Transaction）是一个逻辑工作单元，是指数据库系统中一组对数据的操作序列。

一个事务可以是一条或一组 SQL 语句或整个应用程序。事务具备的以下几个基本特征又称为其应遵循的 ACID 准则：

（1）原子性（Atomicity）。一个事务要么全部执行，要么全不执行，不允许仅完成部分事务。

（2）一致性（Consistency）。事务的正确执行应使数据库从一个一致性状态变为另一个一致性状态。数据一致性是指数据应满足的约束条件。

（3）隔离性（Isolation）。多个事务的并发执行是独立的，在事务未结束前，其他事务不能存取该事务的中间结果数据。

（4）持久性（Durability）。事务提交后，系统应保证事务执行的结果可靠地存放在数据库中，不会因为故障而丢失。

3．并发控制的必要性

同一数据库系统中往往有多个事务并发执行，如果不进行控制，就会产生数据的不一致性，例如出现丢失更新或不可重读的情况。

4．常见的并发控制技术

由上面的介绍可知，为保证数据操作的正确性和一致性，必须进行并发控制。实现并发控制的方法主要有两种：基于封锁的并发控制技术和基于时间戳的并发控制技术。

（1）基于封锁的并发控制技术

基于封锁的并发控制思想是：事务对数据操作前必须获得对该数据的锁，完成操作后在适当时候释放锁；当得不到锁时，事务将处于等待状态。这种技术涉及 3 个方面的问题：

① 封锁协议。系统中的事务在加锁和释放锁时，都必须遵守一组规则，这组规则称为封锁协议。对封锁方式规定不同的规则，就形成了各种不同的封锁协议。前面谈及的丢失更新和不可重读等数据不一致问题，可以通过 3 级封锁协议在不同程度上得到解决。

② 封锁粒度。封锁粒度是指封锁的数据对象的大小。

③ 死锁。一个事务如果申请锁未获准，则须等待其他事务释放锁，这就形成了事务之间的等待关系。当事务中出现循环等待时，如果不加以干预，就会一直等待下去，这种状态称为死锁。基于封锁的并发控制技术需要解决死锁问题，即如何检测、处理和预防死锁。

死锁的检测和处理方法，一般有以下两种。

① 超时法。如果一个事务的等待时间超过某时限，则认为发生死锁。

② 等待图法。等待图是一个有向图，其成图规则是：如果事务 T1 需要的数据已经被事务 T2 封锁，就从 T1 到 T2 画一条有向线段。有向图中出现回路，即表明出现了死锁。发现死锁后，靠事务本身无法打破死锁，必须由数据库管理系统进行干预。

数据库管理系统对死锁一般采用如下策略：

① 在循环等待的事务中，选择一个事务作为牺牲者，给其他事务“让路”。

② 回滚牺牲的事务，释放其获得的锁及其他资源。

③ 将释放的锁让给等待它的事务。

选取牺牲事务的方法有以下几种：

① 选择最迟交付的事务作为牺牲者。

② 选择获得锁最少的事务作为牺牲者。

③ 选择回滚代价最小的事务作为牺牲者。

死锁的预防和检测需要一定的开销，因此要尽量避免死锁的发生。数据库系统中预防死锁常用的方法有以下两种：

① 一次加锁法。一次加锁法是在事务执行前，对要使用的所有数据对象依次加锁并要求加锁成功，只要一个加锁不成功，即表示本次加锁失败，立即释放所有加锁成功的数据对象，然后重新开始加锁。

② 顺序加锁法。顺序加锁法是对所有可能封锁的数据对象按序编号，规定一个加锁顺序，每个事务都按此顺序加锁，释放时则按逆序进行。

（2）基于时间戳的并发控制技术

为了区别事务执行的先后，每个事务在开始执行时，都由系统赋予一个唯一的、随时间增长的整数，称为时间戳（Time Stamp，TS）。设有两个事务 T1 和 T2，如果 TS（T1）<TS（T2），则称 T1 比 T2“年老”或 T2 比 T1“年轻”。

基于时间戳的并发控制思想是：以时间戳的顺序处理冲突，使一组事务的交叉执行等价于一个由时间戳确定的串行序列，其目的是保证冲突的读操作和写操作按照时间戳的顺序执行。

基本的时间戳法遵循以下准则：

① 事务开始时，赋予事务一个时间戳。

② 事务的每个读操作或写操作都带有该事务的时间戳。

③ 对每个数据项 R，记录读过和写过 R 的所有事务的最大时间戳值分别为 RTM(R)和WTM(R)。

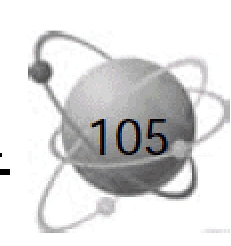
④ 当事务对数据项 R 请求读操作时，若对 R 进行读操作的时间戳为 TS，且 TS<WTM(R)，则拒绝该读操作，并用新的时间戳重新启动该事务；否则，执行读操作，并把 RTM(R)设置成 RTM(R)的最大值。

⑤ 当事务对数据项 R 请求写操作时，若 TS<RTM(R)或 TS<WTM(R)，则拒绝该写操作，并用新的时间戳重新启动该事务；否则，执行写操作，并把 WTM(R)设置为 TS。

在基本时间戳法中，一旦发现冲突，不是等待而是重启事务，因而不会发生死锁，这是其最大优点。但这一优点是以重启事务为代价的，为避免事务重启又有保守时间戳法和乐观的并发控制法等改进方法。

保守时间戳法的基本思想是不拒绝任何操作，因而不必重启事务。如果操作不能执行，则缓冲较年轻事务的操作，直到所有较老的操作执行完为止。此时，系统需要知道什么时候不再有较老的操作存在，而且缓冲事务的操作可能会造成较老事务等待较年轻事务的情况而造成死锁，实现起来比较困难。

乐观的并发控制法是基于事务间的冲突操作很少，因此事务的执行可以不考虑冲突。但为解决冲突写操作，需将其暂时保存，待事务结束后由专门的机构检测是否可以将数据写到数据库中。若不能，则重启该事务。



4.2.4　数据库的备份与恢复

数据库系统如果发生突如其来的故障（例如黑客攻击、病毒袭击、硬件故障和人为误操作等），可能会导致数据的丢失。提高数据的安全性和数据恢复能力一直是用户和厂商关注的焦点。备份是恢复数据最容易和最有效的方法。备份应定期进行，并执行有效的数据管理。

1．数据库的备份

在对数据库进行备份之前，制定相应的备份策略是很有必要的。

（1）制定备份的策略

① 备份周期是按月、周、天还是小时。

② 使用冷备份还是热备份。

③ 使用增量备份还是全部备份，或者两者同时使用。

④ 使用什么介质进行备份，备份到磁盘还是磁带。

⑤ 是人工备份还是设计一个程序定期自动备份。

⑥ 备份介质的存放是否防窃、防磁、防火。

（2）数据库备份的类型

常用的数据库备份的方法有冷备份、热备份和逻辑备份 3 种。

① 冷备份。冷备份是在没有终端用户访问数据库的情况下，关闭数据库并将其备份，又称为“脱机备份”。这种方法在保持数据完整性方面显然最有保障，但是对于那些必须保持每天 24 小时、每周 7 天全天候运行的数据库服务器来说，较长时间地关闭数据库进行备份是不现实的。

② 热备份。热备份是指当数据库正在运行时进行的备份，又称为“联机备份”。因为数据备份需要一段时间，而且备份大容量的数据库也需要较长的时间，那么在此期间发生的数据更新就有可能使备份的数据不能保持完整性。这个问题的解决依赖于数据库日志文件。在备份时，日志文件将需要进行数据更新的指令“堆起来”，并不进行真正的物理更新，因此数据库能被完整地备份。备份结束后，系统再按照被日志文件“堆起来”的指令对数据库进行真正的物理更新。可见，被备份的数据保持了备份开始时刻前的数据一致性状态。

热备份操作存在如下不利因素：

- 如果系统在进行备份时崩溃，则堆在日志文件中的所有事务都会被丢失，即造成数据或更新的丢失。
- 在进行热备份的过程中，如果日志文件占用的系统资源过大，例如将系统存储空间占用完，会造成系统不能接受业务请求的局面，对系统运行产生影响。
- 热备份本身要占用相当一部分系统资源，使系统的运行效率下降。

③ 逻辑备份。逻辑备份是指使用软件技术从数据库中导出数据并写入一个输出文件，该文件的格式一般与原数据库的文件格式不同，只是原数据库中数据内容的一个映像。因此，逻辑备份文件只能用来对数据库进行逻辑恢复，即数据导入，而不能按数据库原来的

存储特征进行物理恢复。逻辑备份一般用于增量备份，即备份那些在上次备份以后改变的数据。

2. 数据库恢复

恢复也称为重载或重入，是指当磁盘损坏或数据库崩溃时，通过转储或卸载的备份重新安装数据库的过程。数据库恢复技术一般有 3 种策略，即基于备份的恢复、基于运行时日志的恢复和基于镜像数据库的恢复。

（1）基于备份的恢复

基于备份的恢复是指周期性地备份数据库，当数据库失效时，可取最近一次的数据库备份来恢复数据库，即把备份的数据复制到原数据库所在的位置上。用这种方法，数据库只能恢复到最近一次备份的状态，而从最近备份到故障发生期间的所有数据库更新将会丢失。备份的周期越长，丢失的更新数据越多。

（2）基于运行时日志的恢复

运行时，可使用日志文件来记录对数据库的每一次更新。对日志的操作优先于对数据库的操作，以确保记录数据库的更改。当系统突然失效而导致事务中断时，可重新装入数据库的副本，把数据库恢复到上一次备份时的状态。然后系统自动正向扫描日志文件，将故障发生前所有提交的事务放到重做队列，将未提交的事务放到撤销队列中执行，这样就可把数据库恢复到故障前某一时刻的数据一致性状态。

（3）基于镜像数据库的恢复

数据库镜像就是在另一个磁盘上复制数据库作为实时副本。当主数据库更新时，DBMS 自动把更新后的数据复制到镜像数据库，始终使镜像数据和主数据保持一致性。当主数据库出现故障时，可由镜像磁盘继续提供使用，同时 DBMS 自动利用镜像磁盘数据进行数据库恢复。镜像策略可以使数据库的可靠性大为提高，但由于数据镜像通过复制数据实现，频繁的复制会降低系统的运行效率，因此一般仅在对效率要求较高的情况下使用。为兼顾可靠性和可用性，可有选择性地镜像关键数据。

数据库的备份和恢复是一个完善的数据库系统必不可少的一部分，目前这种技术已经被广泛应用于数据库产品中。例如，Oracle 数据库提供对联机备份、脱机备份、逻辑备份、完全数据恢复及不完全数据恢复的全面支持。据预测，以“数据”为核心的计算将逐渐取代以“应用”为核心的计算。在一些大型的分布式数据库应用中，多备份恢复和基于数据中心的异地容灾备份恢复等技术正在得到越来越多的应用。

4.3 数据库的安全保护

4.3.1 数据库的安全保护层次

数据库系统的安全除依赖自身内部的安全机制外，还与外部网络环境、应用环境、从

业人员素质等因素息息相关。因此，从广义上讲，数据库系统的安全框架可以划分为 3 个层次——网络系统层次、宿主操作系统层次、数据库管理系统层次。

这 3 个层次构筑成数据库系统的安全体系，与数据安全的关系是逐层紧密的，防范的重要性也逐层加强，从外到内、由表及里保证数据的安全。下面将对安全框架的 3 个层次展开论述。

1. 网络系统层次安全技术

数据库的安全首先依赖于网络系统。随着 Internet 的发展和普及，越来越多的公司将其核心业务向互联网转移，各种基于网络的数据库应用系统如雨后春笋般涌现出来，面向网络用户提供各种信息服务。可以说网络系统是数据库应用的外部环境和基础，数据库系统要发挥其强大作用离不开网络系统的支持，数据库系统的用户（例如异地用户、分布式用户）也要通过网络才能访问数据库中的数据。网络系统的安全是数据库安全的第一道屏障，外部入侵首先就是从入侵网络系统开始的。网络入侵是试图破坏信息系统的完整性、机密性或可信任的任何网络活动的集合，具有以下特点。

- 没有地域和时间的限制，跨越国界的攻击就如同在现场一样方便。
- 借助于网络的攻击往往混杂在大量正常的网络活动之中，隐蔽性强。
- 入侵手段更加隐蔽和复杂。

计算机网络系统在开放式环境中所面临的威胁，主要有以下几种类型。

- 欺骗（Masquerade）。
- 重发（Replay）。
- 报文修改（Modification of Message）。
- 拒绝服务（Deny of Service）。
- 陷阱门（Trapdoor）。
- 特洛伊木马（Trojan Horse）。
- 攻击，如透纳攻击（Tunneling Attack）、应用软件攻击等。

这些安全威胁是无时、无处不在的，因此必须采取有效的措施来保障系统的安全。

从技术角度来讲，网络系统层次的安全防范技术有很多种，大致可以分为防火墙、入侵检测、协作式入侵检测技术等。

（1）防火墙是应用最广的一种防范技术

作为系统的第一道防线，其主要作用是监控可信任网络和不可信任网络之间的访问通道，可在内部与外部网络之间形成一道防护屏障，拦截来自外部的非法访问并阻止内部信息的外泄，但它无法阻拦来自网络内部的非法操作。它根据事先设定的规则来确定是否拦截信息流的进出，但无法动态识别或自适应地调整规则，因而其智能化程度很有限。

（2）入侵检测（Instrusion Detection System，IDS）是近年来发展起来的一种防范技术

入侵检测综合采用了统计技术、规则方法、网络通信技术、人工智能、密码学、推理等技术和方法，其作用是监控网络和计算机系统是否出现被入侵或滥用的征兆。1987 年，Derothy Denning 首次提出了一种检测入侵的思想，经过不断发展和完善，作为监控和识别

攻击的标准解决方案，IDS 系统已经成为安全防御系统的重要组成部分。

2. 宿主操作系统层次

操作系统是大型数据库系统的运行平台，为数据库系统提供了一定程度的安全保护。目前操作系统平台大多数集中在 Windows NT 和 UNIX 上，安全级别通常为 C1、C2 级；主要安全技术包括操作系统安全策略、安全管理策略、数据安全等。

操作系统安全策略用于配置本地计算机的安全设置，包括密码策略、账户锁定策略、审核策略、IP 安全策略、用户权限指派、加密数据的恢复代理以及其他安全选项，具体可以体现在用户账户、口令、访问权限、审计等。

3. 数据库管理系统层次

通过前面两个安全层次的防护，数据库系统的安全性得到了一定程度上的保障，但是这并不意味着危险完全解除。一旦数据库的网络安全层次和操作系统层次被破坏，就需要数据库管理系统层次安全技术来解决问题，这就要求数据库管理系统必须有一套强有力的安全机制。解决这一问题的有效方法之一是数据库管理系统对数据库文件进行加密处理，使得即使数据不幸泄露或者丢失，也难以被人破译和阅读。

4.3.2 数据库的审计

数据库审计是指监视和记录用户对数据库所施加的各种操作的机制。按照美国国防部 TCSEC/TDI 标准中关于安全策略的要求，审计功能是数据库系统达到 C2 以上安全级别必不可少的一项指标。

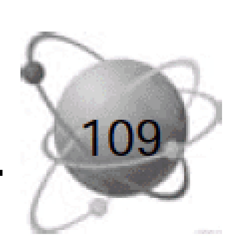
审计功能自动记录用户对数据库的所有操作，并且存入审计日志。事后可以利用这些信息重现导致数据库现有状况的一系列事件，提供分析攻击者线索的依据。

审计功能是数据库管理系统安全性中非常重要的一部分，只要检测审计记录，系统安全员便可掌握数据库被使用的状况。例如，检查库中实体的存取模式，监测指定用户的行为。审计系统可以跟踪用户的全部操作，这也使得审计系统具有一种威慑力，提醒用户安全使用数据库。

数据库管理系统的审计主要分为语句审计、特权审计、模式对象审计和资源审计。语句审计是指监视一个或者多个特定用户或者所有用户提交的 SQL 语句；特权审计是指监视一个或者多个特定用户或者所有用户使用的系统特权；模式对象审计是指监视一个模式中在一个或者多个对象上发生的行为；资源审计是指监视分配给每个用户的系统资源。

审计机制应该至少记录用户标识和认证、客体访问、授权用户进行的影响系统安全的操作，以及其他安全相关事件。对于每个记录的事件，审计记录中需要包括事件发生的时间、用户、时间类型、事件数据和事件的成功/失败情况。对于标识和认证事件，必须记录事件源的终端 ID 和源地址等；对于访问和删除对象的事件，则需要记录对象的名称。

审计的策略库一般由两个方面的因素构成，即数据库本身可选的审计规则和管理员设计的触发策略机制。当这些审计规则或策略机制被触发时，则将引起相关的表操作。这些



表可能是数据库自定义的，也可能是管理员另外定义的，最终这些审计的操作都将被记录在特定的表中以备查证。一般来说，将审计跟踪和数据库日志记录结合起来，会达到更好的安全审计效果。

4.3.3　数据库的加密保护

如果入侵者绕过系统访问数据库的信息内容，如果入侵者通过物理移除磁盘或备份磁盘盗走数据库，如果入侵者接入载有真实用户数据的通信链路，如果聪明的入侵者通过运行程序突破操作系统防线来检索数据，情况会如何呢？

在这些情况下，数据库系统的各种授权规则或许不能提供充分的保护。标准安全技术无法防范绕过系统访问数据的侵扰，这就需要采取其他保护措施来加强系统安全。加密技术提供了附加保护，数据库中的数据是可以被加密的，加密数据是不可能被读出的。加密也构成了鉴定数据库用户身份良好机制的基础。

数据加密是保护数据在存储和传输过程中不被窃取或修改的有效手段。加密的基本思想是根据一定的算法将原始数据（明文）加密成不可直接识别的格式（密文），数据以密文的形式存储和传输。数据加密后，对不知道解密算法和密钥的人，即使通过非法手段访问到数据，也只是一些无法辨认的二进制代码。

1. 常用数据库加密技术

对数据库中的数据进行加密是为了增强普通关系型数据库管理系统的安全性，提供一个安全适用的数据库加密平台，对数据库存储的内容实施有效保护。通过对数据库存储加密等方法可实现数据库中数据存储保密和完整性要求，使得数据库以密文方式存储并在密态方式下工作，确保了数据安全。一般而言，一个行之有效的数据库加密技术主要有以下6个方面的功能和特性。

（1）身份认证。用户除提供用户名、口令外，还必须按照系统的安全性要求提供其他相关安全凭证，例如使用终端密钥。

（2）通信加密与完整性保护。有关数据库的访问在网络传输中都被加密，通信一次一密的意义在于防重放、防篡改。

（3）数据库中数据存储的加密与完整性保护。数据库系统采用数据项级存储加密，即数据库中不同的记录、每条记录的不同字段都采用不同的密钥加密，辅以校验措施来保证数据库中数据存储的保密性和完整性，防止数据的非授权访问和修改。

（4）数据库加密设置。在系统中可以选择需要加密的数据序列，以便于用户选择那些敏感信息进行加密而不是全部数据都加密。只对用户的敏感数据加密，可以提高数据库的访问速度。这样，有利于用户在效率与安全性之间进行自主选择。

（5）多级密钥管理模式。主密钥和主密钥变量保存在安全区域，二级密钥受主密钥变量加密保护，数据加密的密钥存储或传输时利用二级密钥加密保护，使用时受主密钥保护。

（6）安全备份。系统提供数据库明文备份功能和密钥备份功能。

2. 对数据库加密系统的基本要求

（1）字段加密。
（2）密钥动态管理。
（3）合理处理数据。
（4）不影响合法用户的操作。
（5）防止非法复制。

3. 数据加密的算法

加密算法是一些公式和法则，主要用于规定明文和密文之间的变换方法。密钥是控制加密算法和解密算法的关键信息，它的产生、传输、存储等工作是十分重要的。数据加密的基本过程包括对明文（即可读信息）进行翻译，译成密文或密码的代码形式。该过程的逆过程为解密，即将该编码信息转化为其原来的形式的过程。

有关数据加密算法的具体描述参阅第 2 章。

4. 数据加密的实现

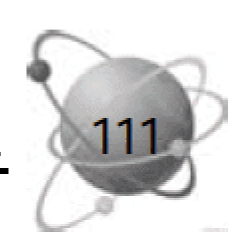
对数据进行加密，主要有 3 种方式，即系统中加密、服务器端（DBMS 内核层）加密、客户端（DBMS 外层）加密。

（1）在系统中加密。在系统中无法辨认数据库文件中的数据关系，将数据先在内存中进行加密，然后文件系统把每次加密后的内存数据写入到数据库文件中，读出时再逆向进行解密。这种加密方法相对简单，只要妥善管理密钥就可以了。其缺点是对数据库的读写都比较麻烦，每次都要进行加/解密的工作，对程序的编写和读/写数据库的速度都会有所影响。

（2）在 DBMS 内核层实现加密，需要对数据库管理系统本身进行操作。这种加密需要数据在物理存取之前完成加/解密工作。这种加密方式的优点是加密功能强，并且加密功能几乎不会影响 DBMS 的功能，可以实现加密功能与数据库管理系统之间的无缝耦合。其缺点是加密运算在服务器端进行，加重了服务器的负载，而且这种加密需要对数据库管理系统本身进行操作，属核心层加密，如果没有数据库开发商的配合，其实现难度相对较大。这种加密方式如图 4-1 所示。

（3）在 DBMS 外层实现加密的好处是不会加重数据库服务器的负载，并且可实现网上的传输。这种加密比较实际的做法是将数据库加密系统做成 DBMS 的一个外层工具，根据加密要求自动完成对数据库中数据的加/解密处理。对那些希望通过 ASP 获得服务的企业来说，只有在客户端实现加/解密，才能保证其数据的安全可靠。这种加密方式如图 4-2 所示。

在这种数据库加密系统中有两个功能独立的重要部件：一个是加密字典管理程序，另一个是数据库加/解密引擎，其体系结构如图 4-3 所示。数据库加密系统将用户对数据库信息具体的加密要求以及基础信息保存在加密字典中，通过调用数据加/解密引擎实现对数据库表的加密、解密及数据转换等功能。数据库信息的加/解密处理是在后台完成的，对数据库服务器是透明的。



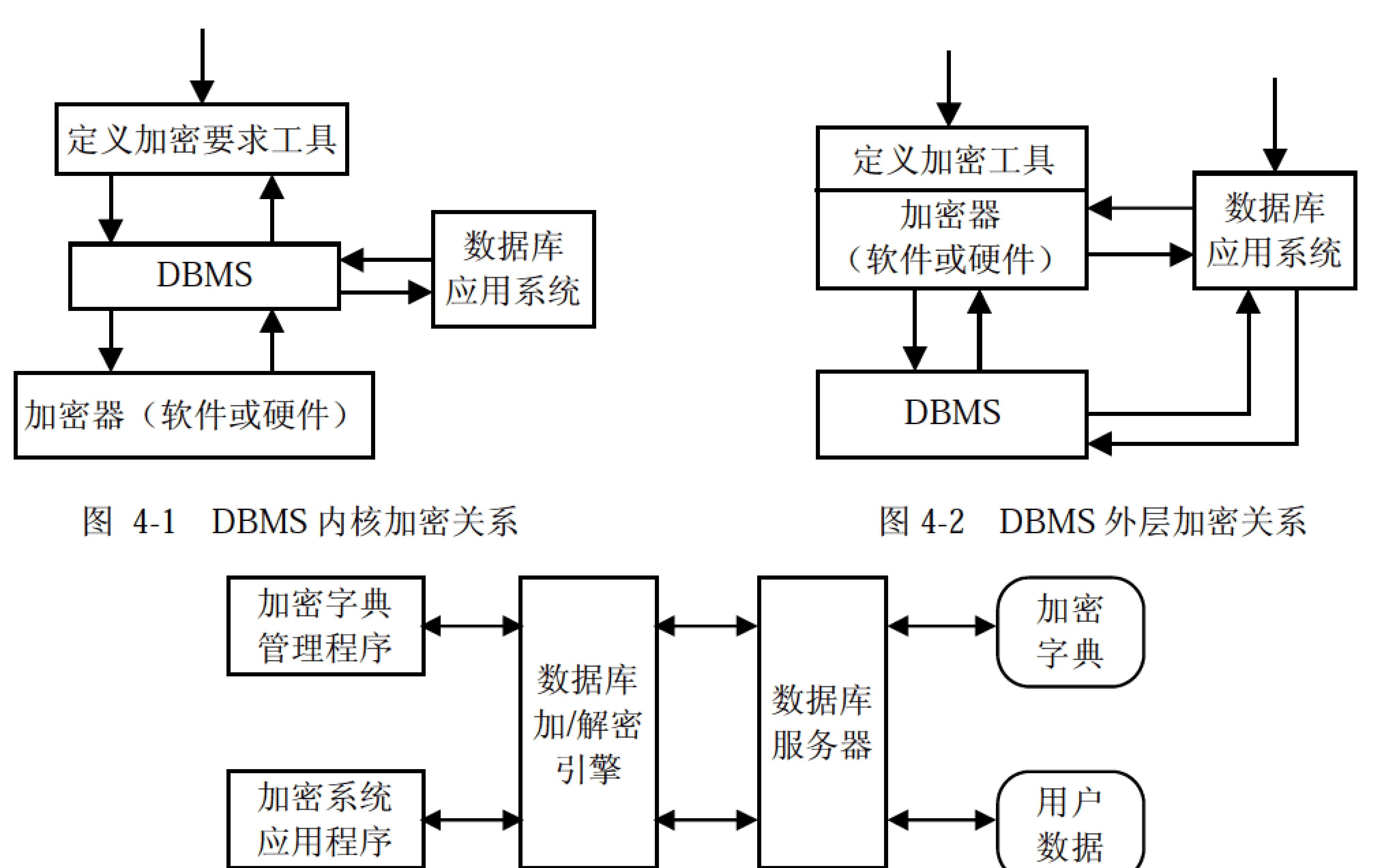


图 4-1 DBMS 内核加密关系

图 4-2 DBMS 外层加密关系

图 4-3 数据库加密系统体系结构

这种数据库加密系统具有很多优点：首先，系统对数据库的最终用户是完全透明的，管理员可以根据需要进行明文和密文的转换工作；其次，加密系统完全独立于数据库应用系统，无须改动数据库应用系统就能实现数据的加密功能；第三，加/解密处理在客户端进行，不会影响数据库服务器的效率。

4.4 Web 数据库的安全

4.4.1 Web 数据库概述

1. Web 数据库的概念

数据库是指按照一定的结构和规则组织起来的相关数据的集合，是存放数据的“仓库”；据此即可将网络数据库定义为以后台数据库为基础的，加上一定的前台程序，通过浏览器完成数据存储、查询等操作的系统。

数据库技术是计算机处理与存储数据的最有效、最成功的技术，而计算机网络的特点是资源共享，因此数据与资源共享这两种技术的结合即成为今天得到广泛应用的 Web 数据库。

Web 数据库的工作流程：首先用户利用浏览器作为输入接口，输入所需要的数据，浏览器随后将这些数据传送给网站，而网站再对这些数据进行处理（例如，将数据存入后台数据库，或者对后台数据库进行查询操作等），最后网站将操作结果传回给浏览器，通过浏览器将结果告知用户。

通常 Web 数据库的环境由硬件元素和软件元素组成。硬件元素包括 Web 服务器、客户机、数据库服务器、网络。软件元素包括客户端必须有能够解释执行 HTML 代码的浏览器，如 IE、Netscape 等；在 Web 服务器中，必须具有可以自动生成 HTML 代码程序的功能，如 ASP、CGI 等；具有能自动完成数据操作指令的数据库系统，如 Access、SQL Server 等。

凭借其易用性、实用性，Web 很快占据了主导地位，并逐渐发展成为目前使用最广泛、最有前途、最有魅力的信息传播技术。不过 Web 服务只是提供了 Internet 上信息交互的平台，随着 Internet 技术的兴起与发展以及 Web 技术的蓬勃发展，人们开始渐渐不满足于只在 Web 浏览器上获取静态的信息，人们需要通过它发表意见、查询数据，甚至进行网上购物，这就迫切需要实现真正的 Internet。

Web 与数据库的互联，将人、企业、社会与 Internet 融为一体。Web 技术发展到今天，人们已经可以把数据库技术引入到 Web 系统中。数据库技术发展比较成熟，特别适用于对大量的数据进行组织管理，而 Web 技术具有较佳的信息发布途径，这两种技术的天然互补性决定了相互融合是其发展的必然趋势。将 Web 技术与数据库技术融合在一起，使数据库系统成为 Web 的重要有机组成部分，不仅可以把二者的所有优点集中在一起，而且能够充分利用大量已有的数据库信息资源，使用户能够在 Web 浏览器上方便地检索和浏览数据库的内容，这对许多软件开发者来说具有极大的吸引力。因此，将 Web 技术与数据库技术相结合，开发动态的 Web 数据库应用已成为当今 Web 技术研究的热点。Web 数据库可以实现方便廉价的资源共享，而数据信息是资源的主体，因而 Web 数据库技术自然而然成为互联网的核心技术。

2. Web 数据库系统的基本模型

Web 数据库的 C/S 和 B/S 模式，分别如图 4-4 和图 4-5 所示。

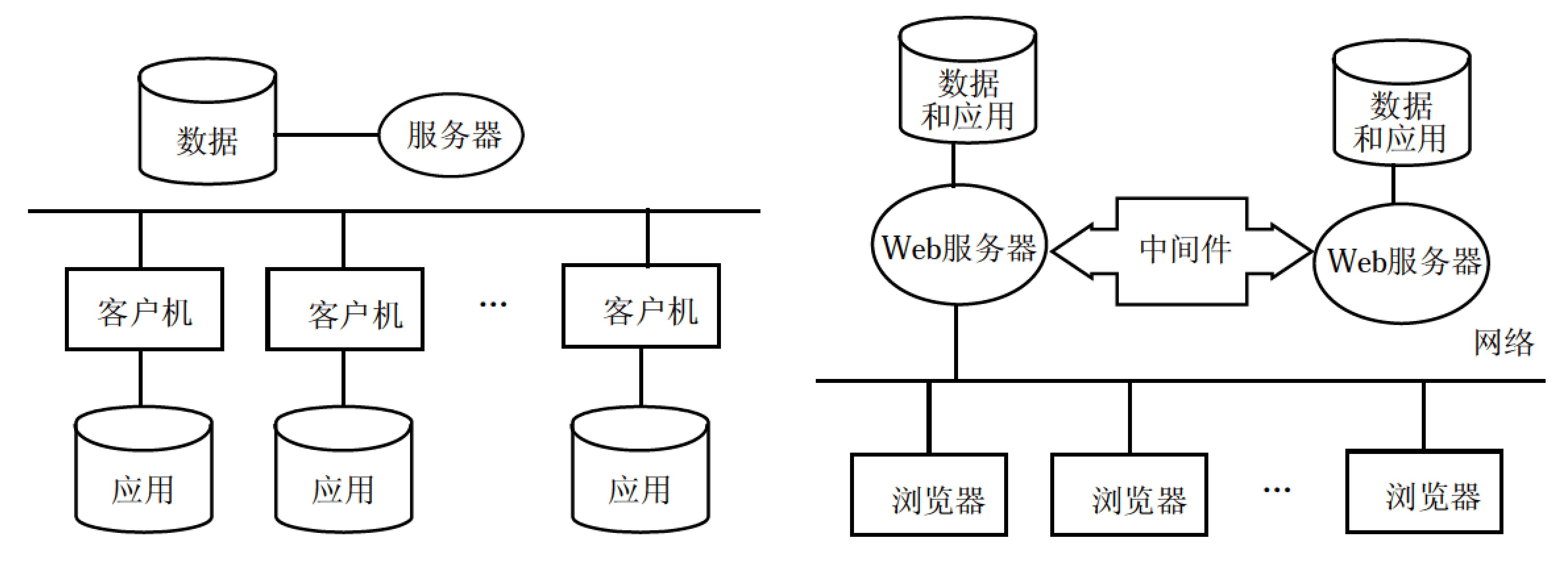
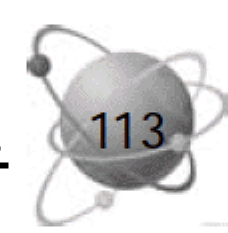


图 4-4 网络数据库的 C/S 模式

图 4-5 网络数据库的 B/S 模式

（1）C/S 模式与 B/S 模式概述

C/S（Client/Server）结构，即客户机/服务器结构。它是软件系统体系结构，通过它可以充分利用两端硬件环境的优势，将任务合理分配到 Client 端和 Server 端来实现，降低了系统的通信开销。目前大多数应用软件系统都是 Client/Server 形式的两层结构。由于现在



的软件应用系统正在向分布式的 Web 应用发展，Web 和 Client/Server 应用都可以进行同样的业务处理，应用不同的模块共享逻辑组件，因此内部的和外部的用户都可以访问新的和现有的应用系统，通过现有应用系统中的逻辑可以扩展出新的应用系统。这便是目前应用系统的发展方向。

B/S（Browser/Server）结构即浏览器/服务器结构。它是随着 Internet 技术的兴起，对 C/S 结构的一种变化或者改进的结构。在这种结构下，用户工作界面是通过 WWW 浏览器来实现的，极少部分事务逻辑在前端即浏览器端实现，主要事务逻辑在服务器端实现。这样就大大简化了客户端电脑负荷，减轻了系统维护与升级的成本和工作量，降低了用户的总体成本。以目前的技术看，局域网建立 B/S 结构的网络应用，尤其是 Internet/Intranet 模式下的数据库应用相对易于把握，成本也较低。它是一次性到位的开发，能实现不同的人员从不同的地点以不同的接入方式访问和操作共同的数据库；可有效地保护数据平台和管理访问权限，服务器上的数据库也很安全。

（2）C/S 与 B/S 模式的区别

① 硬件环境不同。Client/Server 是建立在局域网基础上的，Browser/Server 是建立在广域网基础上的。

② 对安全性要求不同。C/S 模式一般面向相对固定的用户群，对信息安全的控制能力很强。B/S 模式建立在广域网之上，面向不可知的用户群，对安全的控制能力相对比较弱。一般高度机密的信息系统采用 C/S 模式比较适宜，而 B/S 模式适合发布部分可公开信息。

③ 程序架构不同。C/S 程序更加注重流程，可以对权限进行多层次校验，对系统运行速度可以较少考虑；B/S 模式对安全性以及访问速度的多重考虑，建立在需要更加优化的基础之上，比 C/S 模式有更高的要求。

④ 软件重用不同。C/S 构件的重用性不如在 B/S 模式下构件的重用性好。

⑤ 系统维护开销不同。系统维护在软件生存周期中开销大，相当重要。C/S 程序由于整体性，必须整体考察、处理出现的问题以及系统升级困难；B/S 构件组成方面，可以更换个别的构件，实现系统的无缝升级，将系统维护开销减到最小。

⑥ 处理问题不同。C/S 程序可以处理的用户群固定，并且在相同区域，安全性要求高，与操作系统平台相关；B/S 模式建立在广域网上，面向不同的用户群，地域分散，这是 C/S 模式无法做到的，与操作系统平台的联系最少。

⑦ 用户接口不同。C/S 模式多建立在 Windows 平台上，表现方法有限，对程序员普遍要求较高；B/S 模式建立在浏览器上，有更加丰富和生动的表现方式与用户交流，并且大部分难度比较低，开发成本比较低。

⑧ 信息流不同。C/S 程序一般是典型的中央集权的机械式处理，交互性相对比较低；B/S 信息流向可变化，有 B－B、B－C 等信息流向的变化，更像交易中心。

由于以上区别，Web 数据库中的 C/S 模式通过合理的任务分工和协同操作，可以充分发挥数据库服务器和客户机独立的处理功能，在一些大型企业中得到了广泛的应用；而 B/S 模式以其开放、与软硬件平台无关等特点，使其在 Internet 环境中得到了大量的应用。

3. Web 数据库访问技术

Web 页面与数据库的连接是 Web 数据库的基本要求。目前基于 Web 数据库的连接方案主要有两种类型：服务器端和客户端方案。服务器端方案实现技术有 CGI、SAPI、ASP、PHP、JSP 等；客户端方案实现技术有 JDBC（Java Database Connectivity）、DHTML（Dynamic HTML）等。

（1）公共网关接口（Common Gateway Interface，CGI）：Web 服务器运行时外部程序的规范。按照 CGI 编写的程序可以扩展服务器的功能，完成服务器本身不能完成的工作，外部程序执行时可以生成 HTML 文档，并将文档返回 Web 服务器。CGI 程序的常用语言有 Perl、C++、VB、Delphi。其缺点是每个 CGI 程序应用是作为一个独立的外部应用来运行的，与服务器上其他程序竞争处理器资源，这将导致运行速度减慢，同时也不提供状态管理功能，浏览器的每次请求都需要一个连接的建立与释放过程，效率较低。

（2）服务器端应用程序编程接口（Server Application Programming Interface，SAPI）：与 CGI 功能相同，也可用于实现扩展服务器功能。它实际上是一组用于完成特定功能的很复杂的函数、消息和结构，包含在一个扩展名为 DLL 的动态链接库文件中。与 CGI 相比，性能上有了很大的提高，但开发需编程方面的专门知识。

（3）超文本预处理器（Hypertext Preprocessor，PHP）：由于其良好的性能及免费的特点，成为目前互联网中非常流行的一种应用开发平台。其优点是简单易学、跨平台、有良好数据库交换能力的开发语言和良好的安全性。而缺点就是安装配置复杂；缺少企业级的支持；作为自由软件，缺乏正规的商业支持；无法实现商品化的软件开发。

（4）ASP（Activex Server Pages）是由微软创建的 Web 应用开发标准。ASP 服务器已经包含在 IIS 服务器中。ASP 服务器将 Web 请求转入解释器，在解释器中将所有 ASP 中的脚本进行分析，然后执行，同时可以创建 COM 对象以完成更多的功能。ASP 中的脚本语言是 VbScript。其优点是安装和配置方便，开发简单易学，开发工具功能强大；而缺点是 ASP 使用了组件，因而可能会导致大量的安全问题，且无法实现跨平台移植，只能应用于 Windows NT 或 Windows 系统。

4.4.2 常用的几种 Web 数据库

当前比较流行的 Web 数据库主要有：SQL Server、MySQL 和 Oracle。这 3 种数据库适应性强、性能优异、容易使用，在国内得到了广泛的应用。

SQL Server 是微软公司从 Sybase 获得基本部件的使用许可后开发出来的一种关系型数据库。由于均出自微软之手，使得 SQL Server 和 Windows、IIS 等产品有着天然的联系。事实上，以 Windows 为核心的几乎所有微软的软件产品都采用了一致的开发策略，包括界面技术、面向对象技术、组件技术等，这样在微软公司开发的软件中很多都可以相互调用，而且配合得非常密切。因此，如果用户使用的是 Windows 操作系统，那么 IIS、SQL Server 就应该是最佳的选择。

MySQL 是当今 UNIX 或 Linux 类服务器上广泛使用的 Web 数据库系统。它支持大部

分的操作系统平台，设计思想快捷、高效、实用。虽然它对 ANSI SQL 标准的支持并不完善，但支持所有常用的内容，完全可以胜任一般 Web 数据库的工作。由于它不支持事务处理，MySQL 的速度比一些商业数据库快 2～3 倍，并且 MySQL 还针对很多操作系统平台作了优化，完全支持多 CPU 系统的多线程方式。在编程方面，MySQL 也提供了 C、C++、Java、Perl、Python 和 TCL 等 API 接口，而且提供了 MyODBC 接口，任何可以使用 ODBC 接口的语言都可以使用它。更重要的是，MySQL 的源代码是公开的，可以免费使用，这就使得 MySQL 成为许多中小型网站、个人网站追捧的明星。

Oracle 是 Oracle 公司开发的一种面向网络计算机并支持对象—关系模型的数据库产品。它是以高级结构化查询语言为基础的大型关系数据库，是目前最流行的客户/服务器体系机构的数据库之一。

Oracle 之所以备受用户喜爱，是因为它具有以下突出的特点。

（1）支持大型数据库、多用户和高性能的事务处理。Oracle 支持的最大数据库，可达几百千兆，可充分利用硬件设备；支持大量用户同时对数据库执行各种数据操作，并保证数据一致性；系统维护具有很高的性能，Oracle 每天可连续 24 小时工作，正常的系统操作过程中不会中断数据库的应用；可在数据库级或子数据库级上控制数据的可用性。

（2）Oracle 遵循数据库存取语言、操作系统、用户接口和网络通信协议的工业标准，所以它是一个开放系统，保护了用户的投资。美国标准化和技术研究所（NIST）对 Oracle Server 进行过检验，完全与 ANSI/ISO SQL89 标准相兼容。

（3）实施安全性控制和完整性控制。Oracle 为限制系统对各监控数据库的存取提供了可靠的安全性，并为可接受的数据指定标准，保证数据的完整性。

（4）支持分布式数据库和分布式处理。Oracle 为了充分利用计算机系统和网络，允许将处理分为数据库服务器和客户应用程序处理，所有共享的数据管理由数据库管理系统的计算机处理，而运行数据库应用的工作站集中于解释和显示数据。通过网络连接环境，Oracle 将存放在多台计算机上的数据组合成一个逻辑数据库，可被全部网络用户存取。分布式系统像集中式数据库一样具有透明性和数据一致性。

上面介绍的 3 种数据库产品是目前最常用的 3 种大型关系数据库系统，它们虽然在体系结构和操作方法上有许多相似的地方，但是在应用环境上还是各有侧重的。一个应用系统在选用数据库时，性能和价格是首先要考虑的两个因素。从用户的技术水平以及国内软件应用的现状来看，SQL Sever 应该是一个较好的选择。

4.4.3　Web 数据库安全简介

Web 数据库是数据库技术与 Web 技术的结合，其中存在很多安全隐患。例如，通过网络传输的用户名和密码很容易被人窃取，用户读取的数据可能被截取、篡改等。如何保障 Web 数据库的安全运行呢？

要保障 Web 数据库的安全运行，必须从以下几个方面入手，构建一套安全的访问控制模式，如图 4-6 所示。

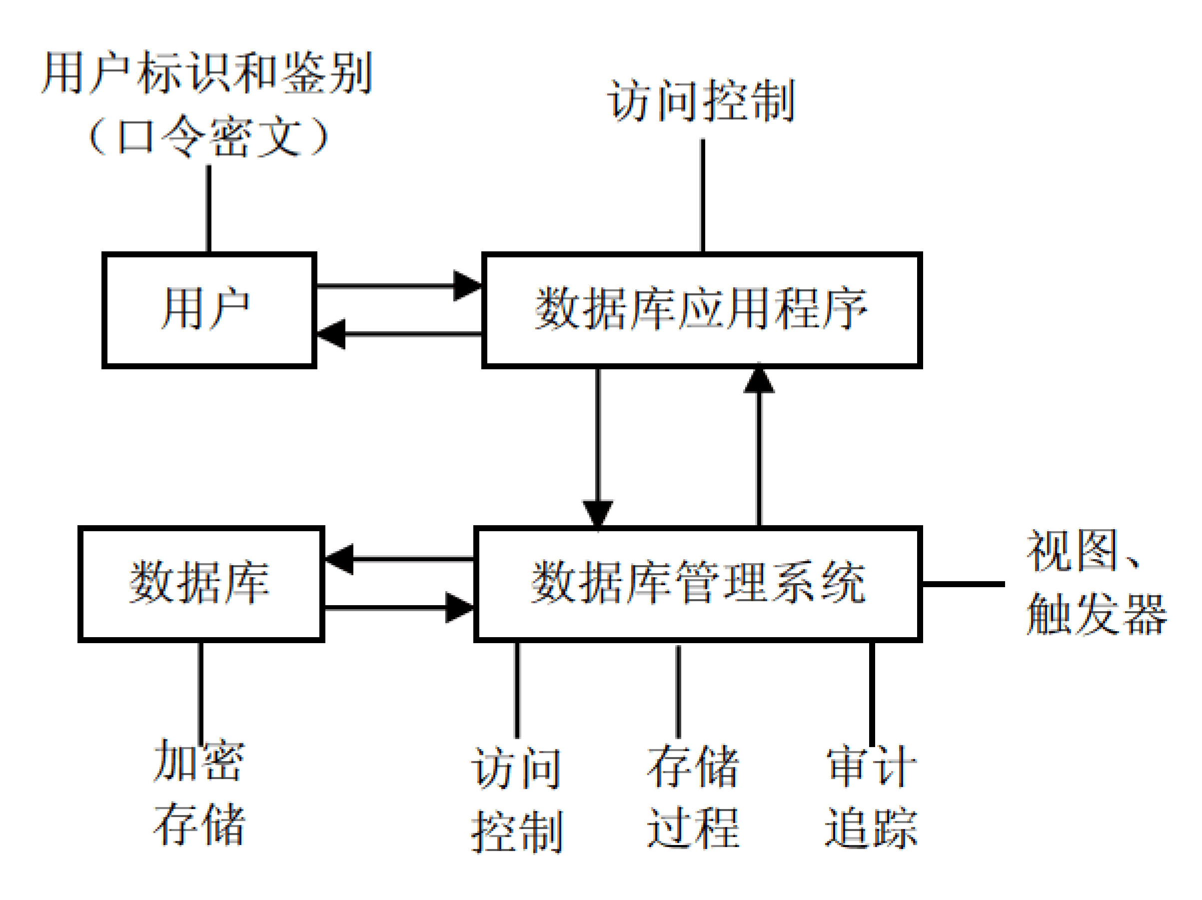


图 4-6　数据库系统安全控制模式

1. 建立安全模型

通常，安全措施贯穿于计算机系统中用户从使用数据库应用程序一直到访问后台数据库所要经过的安全认证过程。当用户访问数据库时，首先通过数据库应用程序进入到数据库系统，这时数据库应用程序会将用户提交的用户名与口令（口令密文）交给数据库管理系统进行认证，在确定其身份合法后，才能进行下一步操作。当要对数据库中的对象（例如表、视图、触发器、存储过程等）进行操作时，也必须通过数据库访问的身份认证，只有通过了数据库的身份认证才能对数据库对象进行实际的操作。

通过身份认证的用户，只是拥有了进入应用系统和数据库的“凭证”，但用户在应用系统和数据库中可以进行什么样的操作，还要依靠“访问控制”和“存取控制”的权限分配和约束。其中“访问控制”与应用系统相关，决定当前用户可以对应用系统中哪些模块、模块中的哪些工作流程进行管理；“存取控制”与数据库相关联，决定当前用户可以对数据库中的哪些对象进行操作，以及可以进行何种操作。虽然“访问控制”和“存取控制”可以将用户的应用系统访问范围最小化、数据对象操作权限最低化，但是就数据库本身而言，利用这种视图、触发器、存储过程等方法来保护数据和对一些敏感数据的“加密存储”也是数据库管理系统提供的安全策略。

2. 审计追踪和数据备份

目前还没有任何一种可行的方法来彻底解决合法用户在通过身份认证后滥用特权的问题，但审计追踪仍是保证数据库安全不可缺少的一道重要防线。

审计是一种监视措施，可跟踪记录有关数据的访问活动。审计追踪把用户对数据库的所有操作自动记录下来，存放在审计日志中。记录的内容一般包括：操作类型（例如修改、查询、删除）、操作终端标识与操作者标识、操作日期和时间以及操作所涉及到的相关数据（例如基本表、视图、记录、属性）等。利用这些信息，可以进一步找出非法存取数据库的人、时间和内容等。

3. 数据库备份恢复策略

计算机同其他设备一样，都可能发生故障。计算机发生故障的原因多种多样，包括磁

盘故障、电源故障、软件故障、灾害故障以及人为破坏等。一旦发生这种情况，就可能造成数据库中数据的丢失。因此，针对数据库系统必须采取必要的措施，以保证发生故障时可以恢复数据库。数据库管理系统的备份和恢复机制就是保证在数据库系统出现故障时，能够将数据库系统还原到正常的状态。

数据备份（建立冗余数据）是指定期或不定期地对数据库进行复制。可以将数据复制到本地机器上，也可以复制到其他机器上。恢复方法通常是利用备份技术、事务日志技术、镜像技术来完成。

4．视图机制和数据加密

为不同的用户定义不同的视图，可以限制各个用户的访问范围。通过视图机制可把要保护的数据对无权存取这些数据的用户隐藏起来，从而自动地对数据库提供一定程度的安全保护。但是视图机制的安全性保护不太精细，往往不能达到应用系统的要求，其主要功能在于提供了数据库的逻辑独立性。在实际应用中，通常将视图机制与授权机制结合起来使用，首先用视图机制屏蔽一部分保密数据，然后在授权机制下进一步定义存取权限。

数据加密是防止数据库中数据在存储和传输中失密的有效手段。加密的基本思想是根据一定的算法将原始数据（明文）加密成不可直接识别的格式（密文），数据以密文的方式存储和传播。

Web 数据库的安全威胁涉及许多方面，是一个全局性的问题，而且黑客的攻击手段和方法不断翻新，因此要根据企业的实际需求综合考虑各种技术，构建一个有机的结合体。同时也要清醒地认识到一个很好的安全解决方案不仅是纯粹的技术问题，而且还需要法律、管理、社会因素的配合。

4.5　SQL Server 数据库的安全

对于数据库管理来说，保护数据不受内部和外部侵害是一项重要的工作。目前比较流行的主流数据库非 Microsoft SQL Server 莫属，下面就来深入地了解一下。

图 4-7 给出了 SQL Server 的安全控制策略示意图。从中可以看到，SQL Server 的安全控制策略是一个层次结构系统的集合，只有满足上一层系统的安全性要求之后，才可以进入下一层。

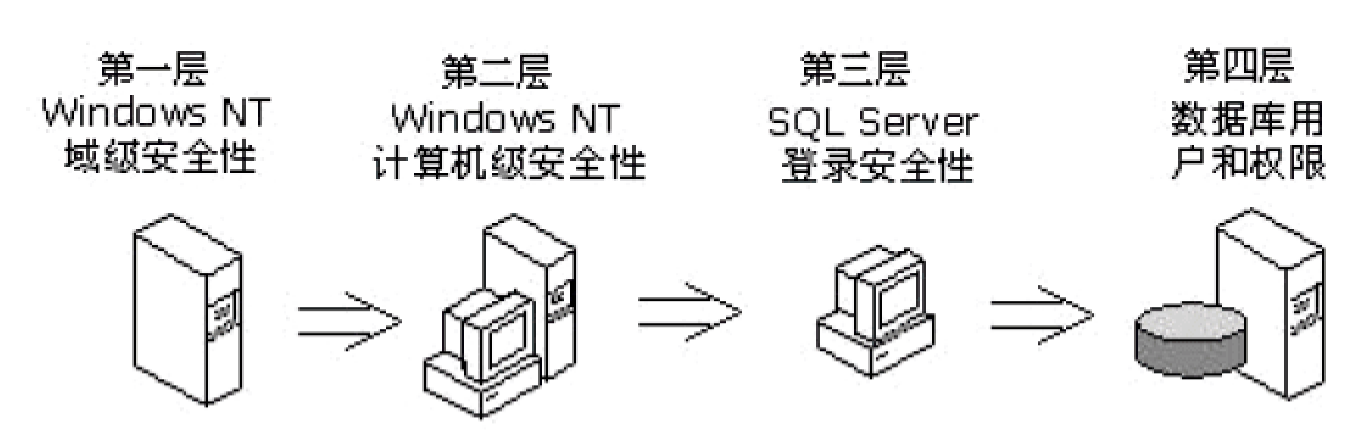


图 4-7　SQL Server 安全性控制策略示意图

各层 SQL Server 安全控制策略是通过各层安全控制系统的身份验证实现的。身份验证

是指当用户访问系统时，系统对该用户的账号和口令的确认过程。身份验证的内容包括确认用户的账号是否有效、能否访问系统、能访问系统的哪些数据等。

身份验证方式是指系统确认用户的方式。SQL Server 系统是基于 Windows NT 或 Windows 操作系统的，现在的 SQL Server 系统安装在 Windows 系统之上（此时将没有第一层和第二层的安全性控制），Windows NT 或 Windows 对用户有自己的身份验证方式，用户必须提供自己的用户名和相应的口令才能访问 Windows NT 或 Windows 系统。

这样，SQL Server 的系统安全可在任何服务器上通过两种方式实现——SQL Server 和 Windows 结合使用以及只使用 Windows。访问 Windows NT 或 Windows 系统的用户能否访问 SQL Server 系统，就取决于 SQL Server 系统身份验证方式的设置。

1. 用户标识与验证

用户标识和验证是系统提供的最外层安全保护措施。其方法是由系统提供一定的方式让用户标示自己的名字或身份。每次用户要求进入系统时，由系统进行核对，通过验证后才提供机器使用权。对于获得上机权的用户，若要使用数据库，数据库管理系统还要进行用户标识和鉴定。

用户标识和验证的方法有很多种，而且在一个系统中往往是多种方法并举，以获得更强的安全性。常用的方法有：

（1）用一个用户名或者用户标识号来标明用户身份。系统内部记录着所有合法用户的标识，用户要求进入系统时，系统将验证此用户是否是合法用户。若是，则可以进入下一步的核实；若不是，则不能使用系统。

（2）为了进一步核实用户，系统常常要求用户输入口令。为保密起见，用户在终端上输入的口令不显示在屏幕上。系统核对口令以验证用户身份。

用户标识与验证在 SQL Server 中对应的是 Windows NT 或 Windows 登录账号和口令以及 SQL Server 用户登录账号和口令。

2. SQL Server 身份验证方式

用户必须使用一个登录账号，才能连接到 SQL Server 中。SQL Server 可以识别两种身份验证方式，即 SQL Server 身份验证方式和 Windows 身份验证方式，如图 4-8 所示。这两种方式都有自己的登录账号类型。

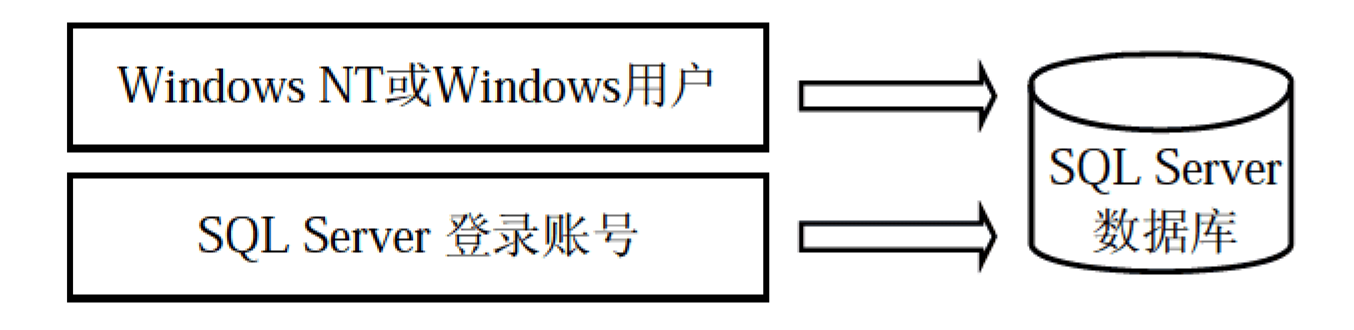
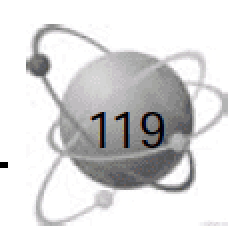


图 4-8 SQL Server 系统身份验证方式示意图

当使用 SQL Server 身份验证方式时，由 SQL Server 系统管理员定义 SQL Server 账号和口令。当用户连接 SQL Server 时，必须提供登录账号和口令。当使用 Windows 身份验证方式时，由 Windows NT 或 Windows 系统管理员决定账号用户对 SQL Server 系统的访问。这



时用户不必提供 SQL Server 的 Login 账号和口令就能连接到系统上，但是在该用户连接之前，SQL Server 系统管理员必须将 Windows NT 或 Windows 账号/组定义为 SQL Server 的有效登录账号。

SQL Server 在 Windows NT 或 Windows 上运行时，系统管理员必须指定系统的身份验证方式。SQL Server 的身份验证方式有两种：Windows 身份验证方式和混合方式。

当使用 Windows 身份验证方式，用户无法以 SQL Server 的登录账号登录服务器。它要求用户登录到 Windows NT 或 Windows，当用户访问 SQL Server 时，不用再次登录。虽然用户仍会被提示登录，但 SQL Server 的用户名会自动从用户网络登录 ID 中提取。这种集成登录只能在用命名管道连接客户机/服务器时使用。

而混合身份验证方式既允许使用 Windows 身份验证方式，又允许使用 SQL Server 身份验证方式。

3. Windows 身份验证方式

Windows 身份验证方式最适用于只在部门访问数据库的情况。与 SQL Server 身份验证方式相比，Windows 身份验证方式具有下列优点。

- 提供了更多的功能，例如安全确认和口令加密、审核、口令失效、最小口令长度和账号锁定。
- 通过增加单个登录账号，允许在 SQL Server 系统中增加用户组。
- 允许用户迅速访问 SQL Server 系统，而不必使用另一个登录账号和口令。

SQL Server 系统按照下列步骤处理 Windows 身份验证方式中的登录账号：

（1）当用户连接到 Windows NT 或 Windows 系统中时，客户机打开一个到 SQL Server 系统的委托连接。该委托连接将 Windows NT 或 Windows 的组和用户账号传送到 SQL Server 系统中。因为客户机打开了一个委托连接，所以 SQL Server 系统知道 Windows NT 或 Windows 已经确认该用户有效。

（2）如果 SQL Server 系统在系统表 syslogins 的 SQL Server 用户清单中找到该用户的 Windows NT 或 Windows 用户账号或者组账号，就接受这次身份验证连接。这时，SQL Server 系统不需要重新验证口令是否有效，因为 Windows NT 或 Windows 已经验证用户的口令是有效的。

（3）在这种情况下，该用户的 SQL Server 系统登录账号既可以是 Windows NT 或 Windows 的用户账号，也可以是 Windows NT 或 Windows 组账号。当然，这些用户账号或者组账号都已定义为 SQL Server 系统登录账号。

（4）如果多个 SQL Server 机器在一个域或者在一组信任域中，那么登录到单个网络域上，就可以访问全部的 SQL Server 机器。

4. 混合方式

混合方式最适合用于外界用户访问数据库或不能登录到 Windows 域时。

混合方式的 SQL Server 身份验证方式有下列优点：混合方式允许非 Windows NT 或 Windows 客户、Internet 客户和混合的客户组连接到 SQL Server 中；SQL Server 身份验证方

式又增加了一层基于 Windows 的安全保护。

SQL Server 按照下列步骤处理自己的登录账号：

（1）当一个使用 SQL Server 账号和口令的用户连接 SQL Server 时，SQL Server 验证该用户是否在系统表 syslogins 中且其口令是否与以前记录的口令匹配。

（2）如果在系统表 syslogins 中没有该用户账号或口令不正确，那么这次身份验证失败，系统拒绝该用户的连接。

SQL Server 提供了多层安全。在最外层，SQL Server 的登录安全性直接集成到 Windows NT 或 Windows 的安全特性中，允许 Windows NT 服务器验证用户。使用这种 Windows 验证，SQL Server 就可以利用 Windows NT 或 Windows 的安全特性，例如安全验证和密码加密、审核、密码过期、最短密码长度，以及在多次登录请求无效后锁定账号。有关 SQL Server 安全性的具体设置方式，可参阅相关书籍，在此不作介绍。

小　　结

本章通过对数据库管理系统的概述，介绍了数据库管理系统存在的各种缺陷，例如账号、密码的泄漏和操作系统后门等。同时，介绍了数据库管理系统面临的数据篡改、损坏和窃取等威胁，说明数据库安全的重要性。通过对数据库安全的重要性和引发数据库安全性问题的分析，提出了用户标识和鉴别、存取控制、用户授权和角色分配等有效的数据库安全控制机制，详细介绍了网络系统、宿主操作系统和数据库管理系统 3 种不同数据库安全保护层次下的保护措施。同时，分析了 Web 数据库安全的重要性，介绍了 Web 数据库的 B/S 和 C/S 两种模型结构，简要介绍了目前主要的 Web 数据库访问技术和常用的几种 Web 数据库，并对广泛应用的 SQL Server 数据库的安全性要求作了简单分析。

练习与思考

1. 什么是数据库的安全性？
2. 试述数据库安全的重要性，说明数据库安全所面临的威胁。
3. 数据库安全性和计算机系统的安全性有什么关系？
4. 试述实现数据库安全控制的常用方法和技术。
5. 什么是数据库中的自主存取控制方法和强制存取控制方法？
6. 数据库中采用了哪些安全技术和保护措施？
7. 常用数据库加密技术有哪几种？
8. 简要介绍 Web 数据库系统的 C/S 和 B/S 基本模型结构。
9. 简述数据备份的方法和策略。
10. 简述 SQL Server 的安全控制策略。

第 5 章

PKI 技术

本章学习要求：

（1）理解口令面临的安全威胁，掌握安全口令的创建和维护。
（2）掌握身份识别与鉴别的概念及身份识别技术，理解生物身份认证技术。
（3）掌握 PKI 的基本概念，了解网络中传输信息的安全要求。
（4）掌握 PKI 的服务功能和实体构成。
（5）掌握 CA 的相关概念、功能和组成。
（6）掌握数字证书的相关概念。
（7）掌握 CA 的密钥管理和 KMC 及时间戳服务。
（8）了解 CA 对数字证书的管理。
（9）了解 PKI 的相关标准。
（10）了解 PKI 的应用。

重点、难点：

（1）重点：身份识别与鉴别的概念及身份识别技术。
（2）难点：数字证书的相关概念、CA 的密钥管理和 KMC 及时间戳服务。

目前，被广泛采用的公钥基础设施（Public Key Infrastructure，PKI）技术采用证书管理公钥，通过第三方的可信任机构——认证中心（Certificate Authority，CA）把用户的公钥和用户的其他标识信息（例如名称、E-mail、身份证号等）捆绑在一起。通过 Internet 的 CA 机构，较好地解决了密钥的分发和管理问题，并通过数字证书，对传输的数据进行加密和鉴别，保证了信息传输的机密性、真实性、完整性和不可否认性。目前，PKI 的安全认证体系得到了各界人士的普遍关注。国外一些大的网络安全公司也都推出了基于 PKI 的产品，例如美国的 VeriSign、IBM 以及加拿大的 Entrust、SUN 等，为用户之间的内部信息交互提供了安全保障。

口令是用于身份标识和身份认证的一种凭证，以密码理论为基础的身份认证和鉴别是访问控制和审计的前提，对网络环境下的信息安全尤其重要，而 PKI 为此提供了全面的解

决方案。本章就从口令和身份认证的基本要领谈起，然后详细介绍 PKI 的相关知识。

5.1 口令安全

口令机制是一种最简单、最常用的系统或应用程序访问控制的方法。因为这种认证用户的方法简单、实现容易而且消耗系统资源少，至今仍在广泛地使用着。随着计算机和网络的日益普及，个人计算机的安全问题变得越来越重要。人们普遍使用口令来限制访问权限；为了提高安全性，必须使用那些难以猜测且难以记忆的口令，在不同的应用（如拨号上网、电子邮件、网站登录 BBS、FTP、各种应用程序等）中使用不同的口令，并在使用过程中频繁更换。用户与大量的口令打交道，随之带来口令的记忆与管理、使用的方便性等一系列问题。口令给用户带来了安全，但同时也增添了不少烦恼。

在当前的网络环境下，系统极其庞大，成百上千台机器之间相互通信，认证类型更加多样化，例如客户机和服务器之间的相互认证、客户机和应用程序间的相互认证；并且在网络环境下，认证的双方一般相隔较远，相互间的信息交流都是明文传输，必然对认证又提出了更高的要求，甚至使用更强的密码算法和更安全的协议。相应地，口令认证也增加了新的要求与内容，如远程口令认证、分布式的口令认证等。网络管理员此时面临的又一负担是大量的口令需要管理。例如，各类用户访问控制策略、方法的选取，所有用户口令机制存在的可能漏洞检测。

5.1.1 口令的管理

几乎所有的计算机及网络系统、通信系统都需要口令，以拥有易于实现的第一级别的访问安全。

非法用户通过一些手段获取口令的过程，称为口令的破解。口令一旦被破解，拥有口令的非法用户即可在网络上做合法用户所做的一切、得到合法用户所能得到的一切。例如，可以冒充合法用户窃取情报或重要数据；以合法用户的身份，冒用信息攻击其他信息系统；修改合法用户的口令，使合法用户无法进入计算机系统或登录；假冒合法用户进行网上交易，挥霍或占有钱财；获得合法用户的个人信息，进行网上诈骗等。总之，将会给合法用户的工作和生活带来许多灾难，甚至造成难以估量的损失。

1．口令安全面临的威胁

尽管目前许多计算机系统和网络的进入或登录都是采用口令来防止非法用户的入侵，然而口令系统却是非常脆弱的。其安全威胁主要来自于：

（1）非法用户利用有问题而缺少保护的口令进行攻击

在计算机系统和网络系统中，用户的口令一般经过加密后将所产生的字符串保存在系统中，当进入系统或登录网络时，用户输入的口令也要进行同样的加密，然后与系统中保存的字符串进行比较。如果相同，则身份认证通过；否则，将会拒绝使用。真正的加密过

程是单向的，无法被逆向解码，也就是说由密文的口令串不能使用逆向算法得到原口令。因此，即便得到了保存在计算机中的口令，也很难获得原口令。然而黑客却可以采用与原加密算法相同的仿真工具，对假设的口令进行加密，再与真实的口令密文进行比较、分析，从而获得口令；或使用口令攻击程序进行试猜来破解口令，常用的手段是使用字典搜索法和蛮力穷举法等。

由于口令都是自然人创建的，人们常常喜欢使用一些特定的词，黑客们便将这些词搜集起来形成口令字典。破解口令时，先用远程主机名找出主机中用户的账号，然后利用口令攻击程序进行试猜，计算机就会自动地从字典中取一个词作为用户口令进行尝试，一个词一个词地循环进行，直至找到正确的口令，这就是字典搜索法。用这种方法破译口令的概率是很大的。如果字典搜索法不能奏效，还可以使用蛮力穷举法，即将口令可能的字符数从小到大，将所有可能的字符进行组合（所有可能的组合），以此为口令进行搜索，进而得到正确的口令。

（2）屏蔽口令

利用一些特殊的程序，跳过口令直接进入系统。

（3）窃取口令

许多网络中，口令在网上的传输是以明文形式发送的，一般的浏览器向 Web 发送消息也是明文的，使得盗窃者很容易得到口令。而有些协议，如 HTTP，即使不是明文，口令的破解也是十分容易的。

（4）木马攻击

木马攻击是指在用户毫无察觉的情况下，黑客将一些特殊的程序趁用户在网络中下载程序或使用电子邮件时安装到用户的计算机中，并使其在无意中执行了这些特殊的程序。这种程序一般具有记录用户的操作信息并将其发送到网上或暂存在硬盘上待用，或直接读取内存或磁盘上口令的功能。例如，BO、Netspy 等就是著名的木马程序。

（5）安全意识淡薄

口令在使用或存储时是很容易泄露的。对一般的用户而言，一方面极少接受过创建或维护口令的安全教育，在选择口令时过于简单，使得破解十分容易；另一方面，缺少保护口令的安全意识，在输入口令时毫无遮掩，旁人可以通过用户的手型和位置猜到，甚至能够直接看到输入的口令；还有就是在保存口令时，喜欢记在纸上或本子里并放在计算机附近，使盗窃口令者极易得到口令。

2. 创建安全口令和维护口令安全

口令对计算机系统和网络系统来说是极为重要的，一个好的口令应该是不容易被破解的，因此创建一个有效的口令是保证其安全的第一步，维护口令安全是第二步。只有二者结合起来，才可以构建一道保护口令安全的防线。

（1）安全口令的创建

从前面口令攻击程序的原理和执行过程可以看出，创建一个有效口令的基本原则如下。

① 口令的长度应尽可能的长，口令字符集中包含的字符应尽可能的多。从数学角度看，若设 m 是口令的长度，n 是字符集的字符数，所有可能的口令总数为 $Y=n^m$，当 n=26、m=6

时，$Y=26^6$。这就是说，如果口令的长度为 6，只用 26 个纯大写或小写字母时，可能的口令总数为 26^6；如果区分字母的大小写，口令的总数为（2×26）^{6}，这时将相差 64 倍；如果 m=8，则口令的总数为（2×26）^{8}，增加到 256 倍。考虑到一个 8 位随机字符的组合数为 3×10^{12} 多种，即便是借助于计算机进行破解，也要很长的时间。因此，口令越长、字符集中的字符数越多，破解需要花费的时间就越多，猜中的概率就越低。

当然，在实际使用中，也不需要太长、字符数很多。因为口令一般是有时限的，假如破解创建的口令需要两个月，而口令时限只有 1 个月，那么这个口令便是有效的，因为当破解者还没有得到该口令时，用户已经更换了新的口令。因此一般可以选择适当长度的口令，口令中应包含字母、数字和其他一些符号。

② 不要选择使用一些有特征的字词作为口令，例如姓名、出生年月日以及常用的英语单词等。口令破解者正是揣摩人们的一般心理，因而在黑客字典中包含了大量的此类单词，很容易破解。

③ 不要选择特别难记的口令，以免遗忘而影响使用。一个理想的有效口令，应该是由计算机动态生成的随机字符串，由于每次出现的字符串都不同，势必增大破解的难度。

④ 最好将创建的口令加密以后，以文件的形式保存在磁盘上，当需要输入口令时，执行一次此文件，这样可以防止盗窃口令者用猜测的方法窃取。

（2）口令安全的维护

创建了一个有效的口令只是做完了一半工作，另一半应该是系统管理员和普通用户的不断维护。系统管理员应该充分利用网络操作系统提供的控制功能，管理和提醒用户保护口令安全。

① 应经常更换口令。这样即使口令被破解了，也可以使用户的损失减少到最小。例如，在 Windows NT 中，系统管理员可以使用“账户规则”对用户口令进行限制——选择“设定口令使用最长期限”项，到时系统会要求用户更改口令；选择“设定最短使用期限”项，限制用户在期限内不能更改口令；选择“设定口令最少字符数”项，系统将要求用户在创建口令时其长度不能少于该数值等。

② 用户不要将自己的口令告诉别人，也不要几个人或几个系统共用一个口令；否则，一旦一个人或一个系统的口令被破解，则所有的口令都将无效。

③ 用户最好不要用电子邮件来传送口令。必须如此时，一定要对邮件进行加密处理，以防止口令在网上被盗窃。同时，用户要尽量减少口令的输入次数，从而减少网上侦听的机会。

④ 当用户使用了难以记忆的口令，应该将记录口令的载体放到远离计算机的地方，以减少被盗窃的机会。

⑤ 用户应增强保护口令的安全意识。

5.1.2　脆弱性口令

口令是系统和个人信息安全的第一道防线。

但是，口令是较弱的安全机制。从责任的角度来看，用户和系统管理员都对口令的失密负有责任，或者说系统管理员和用户两方面都有可能造成口令失密。

脆弱性口令也就是常说的弱口令，易于被破解，在口令设置中不可取。弱口令一般具有下列特征：

（1）系统默认口令。

（2）口令与个人信息相关。

（3）口令为字典中的词语。

（4）过短的口令（口令长度小于或等于 6 位）。

（5）永久性口令。

5.2　身份识别与鉴别

身份鉴别技术在信息安全中处于非常重要的地位，是其他安全机制的基础，是安全系统中的第一道关卡。只有实现了有效的身份鉴别，才能保证访问控制、安全审计、入侵防范等安全机制的有效实施。

5.2.1　身份识别与鉴别的概念

身份识别是指用户向系统出示自己身份证明的过程；身份鉴别是系统核查用户的身份证明的过程，实质上是查明用户是否具有他所请求资源的存储和使用权。人们通常把这两项工作统称为身份鉴别，也称为身份认证。这是判明和确认通信双方真实身份的两个重要环节。身份鉴别必须做到准确无误地将对方辨认出来，同时还应该提供双向的鉴别，即相互证明自己的身份。信息技术领域的身份鉴别通常是通过将一个证据与实体身份绑定来实现的。实体可能是用户、主机、应用程序甚至进程。证据与身份之间是一一对应的关系，双方通信过程中，一方实体向另一方提供这个证据证明自己的身份，另一方通过相应的机制来验证证据，以确定该实体是否与证据所宣称的身份一致。

1. 身份鉴别的任务

计算机系统中的身份鉴别技术一般涉及两方面的内容，即识别和验证。识别信息一般是非秘密的，而验证信息必须是秘密的。所谓“识别”，就是要明确访问者是谁，即识别访问者的身份，且必须对系统中的每个合法用户都有识别能力。要保证识别的有效性，必须保证任意两个不同的用户都不能具有相同的标识符，通过唯一标识符 ID，系统可以识别出访问系统的每一个用户。所谓“验证”，是指在访问者声明自己的身份（向系统输入它的标识符）后，系统必须对它所声明的身份进行验证，以防假冒，实际上就是证实用户的身份。验证过程中用户必须出具能够证明他的身份的特殊信息，这个信息是秘密的，任何其他用户都不能拥有。只有识别与验证过程都正确后，系统才会允许用户访问系统资源。

身份鉴别的目的是验证信息收发方是否持有合法的身份认证符（口令、密钥和实物证

件等）。从认证机制上讲，身份认证技术可分为两类：一类是专门进行身份认证的直接身份认证技术；另一类是在消息签名和加密认证过程中，通过检验收发方是否持有合法的密钥进行的认证，称为间接身份认证技术。

在用户接入（或登录）系统时，直接身份认证技术要首先验证他是否持有合法的身份证（口令或实物证件等）。如果他有合法的身份证，就允许他接入到系统中，进行允许的收发等操作；否则，拒绝他接入到系统中。通信和数据系统的安全性常常取决于能否正确识别通信用户或终端的个人身份。例如，银行的自动取款机 ATM 可将现款发放给经它正确识别的账号持卡人。对计算机的访问和使用及安全地区的出入、放行等都是以准确的身份认证为基础的。

2. 身份鉴别技术

通常有 3 种方法来验证主体身份：一是只有该主体了解的秘密，例如口令、密钥；二是主体携带的物品，例如智能卡和令牌卡；三是只有该主体具有的独一无二的特征（人体测量学或生物统计学方面）或能力，如脸像、虹膜、指纹、掌纹、声音、步态或笔迹等。

（1）口令机制

口令是相互约定的代码，只有用户和系统知道。口令可以由用户自己选择，也可以由系统分配。通常情况下，用户先输入某种标志信息，例如用户名和 ID 号，然后系统询问用户口令，若口令与系统保存的用户文件中的相匹配，用户即可进入系统。

这是目前在互联网和计算机领域中最常用的鉴别方法，当你登录计算机网络时需要输入口令。计算机系统把它的鉴别建立在用户名和口令的基础之上，如果你把用户名和口令告诉了其他人，则计算机也将给予那个人以访问权限，因为鉴别是建立在已知口令之上的，仅仅属于一种模式的鉴别。通过一些措施可以有效地改进口令鉴别的安全性，例如增加口令的强度，提高抗穷举攻击和字典攻击的能力；将口令加密，防止在传输中被窃听；采用动态的一次性口令等。

（2）智能卡

访问不但需要口令，还需要使用物理智能卡，在允许进入系统之前检查是否允许接触系统。智能卡大小如信用卡（国内已经出现形如 U 盘且具 USB 接口的认证设备），一般由微处理器、存储及输入/输出设备构成。微处理器可计算该卡的一个序列号 ID 和其他数据的加密形式，ID 只要保证智能卡的真实性，持卡人就能访问系统。为防止智能卡遗失或被窃，许多系统需要卡和身份识别码 PIN 同时使用，若仅有卡而不知道密码，则不能进入系统。基于智能卡的认证方式是一种双因素的认证方式（PIN+智能卡），即使 PIN 或智能卡被窃取，用户仍不会被冒充。智能卡提供硬件保护措施和加密算法，可以利用这些功能加强安全性能。例如，可以把智能卡设置成用户只能得到加密后的某个秘密信息，从而防止秘密信息的泄露。智能卡比传统的口令方法鉴别能力更强，但其携带不方便，且开户费用较高。

（3）主体特征鉴别

这种认证方式以人体唯一的、可靠的、稳定的生物特征（例如指纹、虹膜、脸部、掌

纹等）为依据，采用计算机的强大功能和网络技术进行图像处理和模式识别。该技术具有很好的安全性、可靠性和有效性，与传统的身份确认手段相比，产生了质的飞跃。利用生物学特征的身份验证机制提供了很高的安全性，但其生物特征信息采集、认证装备的成本较高，只适用于安全级别比较高的场所。另外，软件方面需进一步降低误识率，不断提高身份认证的正确性、准确性。

5.2.2　身份鉴别的过程

认证技术是保障网络安全的重要手段。用户认证系统主要是通过数字认证技术确认用户的身份，从而提供相应的服务。决定身份真实性的身份鉴别过程包括如下两个步骤：

（1）为实体赋予身份，并绑定身份，决定身份的表现方式

身份的赋予必须由具有更高优先权的实体进行。这些被充分信任的实体可通过类似于驾照检查或指纹验证等办法，来确定实体的真实性，随后赋予真实实体相应的身份信息。

每个实体的身份信息应当是独一无二的，同时身份信息要能被对等的其他实体所理解。目前可采用如下方式完成身份的赋予和表示：系统管理员为用户提供账号和口令；网络管理员为每台机器赋予 IP 地址；分配对称密钥的方法；分配公钥/私钥的方法；产生公钥的证书授权方法；安全人员建立名字和指纹序列的联系；身份的可信度取决于验证身份正确性的过程和实施身份赋予和绑定实体的真实性。

可靠的身份认证，是保护网络系统免受诸如伪装和内部人员修改攻击等破坏的第一步。

（2）通信与鉴别

对实体的访问请求，必须鉴别其身份。认证的基本模式可分为 3 类：

① 用户到主机：当用户登录到主机或工作站时，用户对主机和网络的访问首先必须经过身份认证过程。最佳方法是综合采用多种认证方式，例如口令、物理令牌和生物方法的验证。

② 点对点认证：认证双方通过认证协议互相通信，获得对方的认证信息，完成身份认证工作。

③ 第三方的认证：由充分信任的第三方提供认证信息。在这种模式下，保证第三方的可信度非常重要。建立和维护第三方信任度，要求制定关于出具证书的规则和过程，确保认证过程的数据完整性，使用安全的通信协议与认证服务器进行通信。

认证可采用的机制，应分成简单和加密两种类型。简单的认证机制，通过比较被认证实体提供的信息和本地存储的对应信息来实现；而基于加密的认证机制，则建立在加密协议对数据的加密处理的基础上。通信双方可能持有公共的密钥（通常存储在硬件的令牌里），从而实现质询/应答的协议，完成认证。其他机制，可以只是基于公钥和公钥同公钥证书之间的对应关系。例如，身份是本地定义的名字，所有可能参与通信的对象的名字都在本地的一个把它们的身份同其公钥联系起来的可信的数据库当中，使用所存储的公钥验证数字签名，就可以实现身份的鉴别。

5.2.3 生物身份认证

生物特征身份鉴别技术是通过计算机收集人体所固有的生理或行为特征并进行处理，由此进行个人身份鉴定的技术。

并非所有的生物特征都可用于个人的身份鉴别。身份鉴别可利用的生物特征必须满足以下几个条件：

- 普遍性：即每个人都必须具备这种特征。
- 唯一性：即任何两个人的特征是不一样的。
- 可测量性：即特征可测量。
- 稳定性：即特征在一段时间内不改变。

当然，在应用过程中，还要考虑其他的实际因素，如识别精度、识别速度、对人体无伤害、被识别者的接受性等。

目前，研究和使用的生物特征包括脸部、虹膜、视网膜、指纹、掌纹和手形等与生俱来的生理特征和语音、签名、步态等后天习惯使然的行为特征。

1. 基于生理特征的识别技术

（1）指纹识别

指纹是指手指末梢乳突纹凸起形成的纹线图案，其稳定性、唯一性早已获得公认。目前指纹识别技术主要是利用指纹纹线所提供的细节特征（即纹线的起、终点、中断处、分叉点、汇合点、转折点）的位置、类型、数目和方向的比对来鉴别身份。指纹识别在所有生物特征识别技术中，无论从硬件设备还是软件算法上都是最成熟、应用最早、使用最广泛的。尽管如此，指纹识别技术也有不足之处，对指纹质量较差的人群，如皮肤干燥、有疤痕、老茧、表面磨损严重和有病变的人无法取得好的识别效果，因为指纹使用接触式采集。

（2）虹膜识别

虹膜是指位于瞳孔和巩膜间的环状区域，每个人虹膜上的纹理、血管、斑点等细微特征各不相同，且一生中几乎不发生变化。用摄像机捕获用户眼睛的图像，从中分割出虹膜图像，即可进行定位校准、特征提取、编码用以匹配。到目前为止，虹膜识别的错误率是各种生物特征识别技术中最低的。但虹膜因受到眼睑、睫毛的遮挡，准确捕获虹膜图像很困难，图像采集设备复杂昂贵，且虹膜一旦有病变或损伤会影响识别，对盲人和患有如白内障等眼部疾病的人无效。

（3）视网膜识别

人体的血管纹路也是具有独特性的。人的视网膜上血管的图样可以利用光学方法透过人眼晶体来测定。用于生物识别的血管分布在神经视网膜周围，即视网膜 4 层细胞的最远处。如果视网膜不被损伤，从 3 岁起就会终身不变。同虹膜识别技术一样，视网膜扫描可能是最可靠、最值得信赖的生物识别技术，但应用难度较大——视网膜识别技术要求激光

照射眼球的背面以获得视网膜特征的唯一性。

视网膜技术的优点是：视网膜是一种极其固定的生物特征，因为它是“隐藏”的，故而不易磨损、老化或是为疾病影响；非接触性的；视网膜是不可见的，故而不会被伪造。缺点是：视网膜技术未经过任何测试，可能会给使用者带来健康危害，这需要进一步的研究；对于消费者，视网膜技术没有吸引力；很难进一步降低它的成本。

（4）面部识别

面部识别技术通过对面部特征和它们之间的关系（眼睛、鼻子和嘴的位置以及它们之间的相对位置）来进行识别。用于捕捉面部图像的技术有两种，即标准视频技术和热成像技术。标准视频技术通过视频摄像头摄取面部的图像，而热成像技术通过分析由面部毛细血管中的血液产生的热线束产生面部图像。与视频摄像头不同，热成像技术并不需要较好的光源，即使在黑暗的情况下也可以使用。

面部识别技术的优点是：非接触性的。其缺点是：要用比较高级的摄像头才可有效、高速地捕捉面部图像；使用者面部的位置与周围的光环境都可能影响系统的精确性，而且面部识别也是最容易被欺骗的；另外，对于人体面部、头发、饰物、变老以及其他的变化可能需要通过人工智能技术来得到补偿；用于采集图像的设备会比其他技术昂贵得多。这些因素限制了面部识别技术广泛地运用。

（5）手形识别

手形识别技术主要是利用手掌、手指及手指各关节的长、宽、厚等三维尺寸和连接特征来进行身份鉴别。这些特征采集简单，不易受噪声干扰，对设备要求不高，其识别速度在所有生物特征识别系统中是最快的；但因识别率相对较低，一般只用于身份验证。手形识别系统使用方便，价格合理，已在机场、海关、高级住宅、进出口控制等方面得到广泛应用，市场占有量仅次于指纹识别系统。不过，当手部因劳动、外伤或疾病等原因造成外形上的变化时，会影响系统鉴别的准确性。

（6）红外温谱图

人的身体各个部位都在向外散发热量，而每个人的生物特征都不同，从而导致其发热强度不同。此时通过红外设备即可获得反映身体各个部位发热强度的图像，这种图像称为温谱图。拍摄温谱图的方法和拍摄普通照片的方法类似，因此可以用人体的各个部位来进行鉴别。例如，可对面部或手背静脉结构进行鉴别来区分不同的身份。温谱图的数据采集方式决定了其可以用于隐蔽的身份鉴定。除了用来进行身份鉴别外，温谱图的另一个应用是吸毒检测。因为人体服用某种毒品后，其温谱图会显示特定的结构。温谱图的方法具有可接受性，因为数据的获取是非接触式的，具有非侵犯性。但是，人体的温谱值受外界环境影响很大，对于每个人来说不是完全固定的。目前，已经有温谱图身份鉴别的产品，但是由于红外测温设备的昂贵价格，使得该技术不能得到广泛的应用。

（7）语音识别

语音识别利用说话者发声频率和幅值的不同来辨识身份。语音识别大体分两类：一是依赖特定文字识别，例如让说话者说某个特定的词语或几个特定词语中随机的某个来识别真伪，这种方式系统设计简单，较易实现，但安全性较差；另一种是不依赖特定文字识别，

即说话者可随意说任何词语，由系统找出说话者发音中具有共性的特征进行识别，该方式虽有很好的防伪性，但系统复杂，实现起来存在一定困难。因语音远程传递的方便性，在电话拨号系统中该方法具有其他生物特征识别技术不可取代的优势，但也存在较多不足。例如，语音受心理状态、疾病等自身因素和语音环境、采集设备、传输通道等外部因素的干扰，会影响识别效果，使用磁带录音进行欺诈的可能性也未能很好地解决。

（8）味纹识别

人的身体是一种味源，人类的气味虽然会受到饮食、情绪、环境、时间等因素的影响和干扰，其成分和含量会发生一定的变化，但作为由基因决定的那一部分气味——味纹却始终存在，而且终生不变，可以作为识别任何一个人的标记。

由于气味的性质相当稳定，如果将其密封在试管里制成气味档案，可以足足保存 3 年，即使是在露天空气中也能保存 18 小时。科学家告诉我们，人的味纹从手掌中可以轻易获得。首先将手掌握过的物品，用一块经过特殊处理的棉布包裹住，放进一个密封的容器，然后通入氮气，让气流慢慢地把气味分子转移到棉布上，这块棉布就成了保持人类味纹的档案。可利用训练有素的警犬或电子鼻识别不同的气味。

（9）基因 DNA 识别

脱氧核糖核酸 DNA 存在于一切有核的动（植）物中，生物的全部遗传信息都储存在 DNA 分子里。由于不同的人体细胞中具有不同的 DNA 分子结构，且在整个人类范围内具有唯一性和永久性，因此除了对双胞胎个体的鉴别可能失去它应有的功能外，这种方法具有绝对的权威性和准确性。不像指纹必须从手指上提取，DNA 模式在身体的每一个细胞和组织都一样。这种方法的准确性优于其他任何生物特征识别方法，广泛应用于识别罪犯。它的主要问题是使用者的伦理问题和实际的可接受性，DNA 模式识别必须在实验室中进行，不能达到实时以及抗干扰；耗时长是另一个问题。这就限制了 DNA 识别技术的使用。另外，某些特殊疾病可能改变人体 DNA 的结构，系统无法对这类人群进行识别。

2. 基于行为特征的生物识别技术

（1）步态识别

步态是指人们行走时的方式，这是一种复杂的行为特征。步态识别主要提取的特征是人体每个关节的运动。尽管步态不是每个人都不相同的，但是也可提供充足的信息来识别人的身份。步态识别的输入是一段行走的视频图像序列，因此其数据采集与面部识别类似，具有非侵犯性和可接受性。但是，由于序列图像的数据量较大，因此步态识别的计算复杂性比较高，处理起来也比较困难。尽管生物力学中对于步态进行了大量的研究工作，但基于步态的身份鉴别研究工作刚刚开始，到目前为止，还没有商业化的基于步态的身份鉴别系统。

（2）击键识别

这是基于人击键时的特性，如击键的持续时间、击不同键之间的时间间隔、出错的频率以及力度大小等而达到进行身份识别的目的。20 世纪 80 年代初期，美国国家自然科学基金会和国家标准局研究证实，击键方式是一种可以被识别的动态特征。

（3）签名识别

签名识别是日常生活中我们接触最多的一种身份识别方法，接受程度高。签名作为身份认证的手段已经用了几百年了，对此我们非常熟悉，如在银行的格式表单中签名作为我们身份的标志。将签名数字化是这样一个过程：测量图像本身以及整个签名的动作在每个字母以及字母之间的不同速度、顺序和压力。

签名识别按获取方式分为离线和在线识别两种。离线识别通过扫描仪获取已书写好的文字图像，利用计算机从中提取文字的几何特征，由笔画本身特征和相互关系来进行识别。这种方式简单，但易被伪造。在线识别需用专用手写板和压敏笔来记录整个书写过程，包括书写的笔画顺序、笔尖压力、倾斜度及书写时的速度和加速度等丰富的动态特性，弥补了离线识别只取静态特性的不足，难以伪造。

签名识别易被大众接受，是一种公认的身份识别的技术。但事实表明人们的签名在不同的时期和不同的精神状态下是不一样的，这就降低了签名识别系统的可靠性。

5.3　PKI 概述

公钥基础设施 PKI，是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务具有普遍性的安全基础设施。该体系在统一的安全认证标准和规范基础上提供了在线身份认证，是 CA 认证、数字证书、数字签名以及相关的安全应用组件的集合。PKI 的核心是解决信息网络空间中的信任问题，确定信息网络、信息空间中各种经济、军事和管理行为的主体（包括组织和个人）身份的唯一性、真实性和合法性，为组织机构建立和维护一个可信赖的系统环境，透明地为应用系统提供身份认证、数据保密性和完整性、抗抵赖等各种必要的安全保障，满足各种应用系统的安全需求。

PKI 产生于 20 世纪 80 年代，是一种遵循既定标准的密钥管理平台，能够为所有网络应用提供加密和数字签名等密码服务及必需的密钥和证书管理体系。它采用证书管理公钥，通过第三方的可信任机构——认证中心（Certificate Authority，CA），把用户的公钥和其他标识信息捆绑在一起，在 Internet 网上验证用户身份。

目前，PKI 技术已逐渐覆盖了从安全电子邮件、虚拟专用网络 VPN、Web 交互安全到电子商务、电子政务、电子事务安全等众多领域。毫无疑问，PKI 作为一种安全基础设施，在提供安全的网络应用方面，较某些技术措施更具全局性，发挥着更重要的作用。

5.3.1　PKI 的概念、目的、实体构成和服务

1．PKI 的概念

（1）PKI 的定义

PKI 是一个用公钥概念与技术来实施和提供安全服务的普遍适用的安全基础设施。

PKI 是一个为综合数字信息系统提供广泛需要的加密和数字签名服务的基础设施，其

主要职责是管理密钥和证书，建立和维护一个值得信任的网络环境。PKI 能够为跨越各种领域的广泛应用提供加密和数字签名服务。

PKI 是由认证机构、策略和技术标准、必要的法律组成。

（2）PKI 原理

公共（非对称）密钥算法使用加密算法和一对密钥——一个公钥和一个私钥。其基本原理是：由一个密钥进行加密的信息内容，只能由与之配对的另一个密钥才能进行解密。公钥可以广泛地发给与自己有关的通信者，私钥则需要十分安全地存放起来。使用中，甲方可以用乙方的公钥对数据进行加密并传送给乙方，乙方可以使用自己的私钥完成解密。公钥通过电子证书与其拥有者的姓名、工作单位、邮箱地址等捆绑在一起，由权威机构认证、发放和管理。将证书交给对方时，也就把自己的公钥传送给了对方。证书也可以存放在一个公开的地方，让别人能够方便地找到和下载。

公共密钥方法还提供了进行数字签名的方法：签字方对要发送的数据提取摘要并用自己的私钥对其进行加密；接收方验证签字方证书的有效性和身份，用签字方公钥进行解密和验证，确认被签字的信息的完整性和抗抵赖性。

（3）PKI 的安全服务功能

PKI 的主要功能是提供身份认证、机密性、完整性和不可否认性服务。

① 身份认证。信息的接收者应该能够确认信息的来源，使得交易双方的身份不能被入侵者假冒或伪装。

因为公钥是公开的，需要在网上传输，如何对其进行管理便成为 PKI 系统的关键问题。目前较好的解决方案是引进证书机制。证书是公开密钥体制的一种密钥管理媒介。它是一种权威性的电子文档，形同网络计算环境中的一种身份证，用于证明某一主体（例如人、服务器等）的身份以及其公开密钥的合法性。PKI 通过证书进行认证。证书是一个可信的第三方证明，通过它，通信双方可以安全地进行相互认证而不用担心别人会假冒自己。

② 机密性。确保一个计算机系统中的信息和被传输的信息仅能被授权读取的各方得到。

PKI 基础设施采用证书管理公钥，通过第三方的可信任机构——认证中心 CA，把用户的公钥和用户的其他标识信息捆绑在一起，在 Internet 上验证用户的身份；PKI 将公钥密码和对称密码结合起来，在 Internet 上实现密钥的自动管理，确保网上数据的安全传输。

③ 信息的完整性。信息的完整性就是防止非法篡改信息，例如修改、复制、插入和删除等。在交易过程中，要确保交易双方接收到的数据和从数据源发出的数据完全一致，数据在传输和存储的过程中不能被篡改，否则交易将无法完成或所做交易违背交易意图。

在国内 PKI 体系所实现的方案中，目前通常采用 SHA-1、MD-5、Hash 等标准散列算法来保证数据的完整性。在实际应用中，通信双方通过协商以确定使用的算法和密钥，从而在两端计算条件一致的情况下，对同一数据计算出相同的结果来保证数据不被篡改，实现数据的完整性。

④ 信息的不可否认性。不可否认用于从技术上保证实体对他们行为的诚实，即参与交互的双方都不能事后否认自己曾经处理过的每笔业务。在这中间，人们更关注的是数据来

源的不可否认性、发送方的不可否认性，以及接收方在接收后的不可否认性。此外，还有传输的不可否认性、创建的不可否认性和同意的不可否认性等。PKI 所提供的不可否认功能，主要是基于数字签名及其所提供的时间戳服务功能。

在进行数字签名时，签名私钥只能被签名者自己掌握，系统中的其他参与实体无法得到该密钥，进而只有签名者自己能做出相应的签名，其他实体是无法做出这样的签名的。这样，签名者从技术上也就不能否认自己做过该签名。为了保证签名私钥的安全，一般要求这种密钥只能在防篡改的硬件令牌上产生，并且永远不能离开令牌。

PKI 提供的安全时间戳服务用来证明某个特别事件发生在某个特定的时间或某段特别数据在某个日期已存在。这样，签名者对自己所做的签名将无法进行否认。

（4）PKI 的特点

PKI 是以公钥概念与技术来提供具有通用性的安全服务，应以商业驱动而不是以技术为中心来实施 PKI 计划。其特点是：

① 节省费用。在一个大型的应用系统中，实现统一的安全解决方案，比实施多个有限的解决方案，费用要少得多。

② 互操作性。在一个系统内部，实施多个点对点的解决方案，无法实现互操作性。在 PKI 中，每个用户程序和设备都以相同的方式访问和使用安全服务功能。

③ 开放性。任何先进技术的早期设计，都希望在将来能和其他系统间实现互操作，而一个专有的点对点技术方案不能处理多域间的复杂性，不具有开放性。

④ 一致的解决方案。一致解决方案在一个系统内更易于安装、管理和维护，并且开销小。

⑤ 可验证性。PKI 在所有应用系统和设备之间所采用的交互处理方式都是统一的，因此其操作和交互都可以被验证是否正确。

⑥ 可选择性。PKI 为管理员和用户提供了许多可选择性。

2. PKI 的目的

从广义上讲，任何提供公钥加密和数字签名服务的系统，都可叫做 PKI 系统，PKI 的主要目的是通过自动管理密钥和证书，能够为用户建立起一个安全的网络运行环境，使用户能够在多种应用环境下方便地使用加密和数字签名技术，从而确保网上数据的机密性、完整性、有效性。一个有效的 PKI 系统必须是安全的和透明的，用户在获得加密和数字签名服务时，无需周详地了解 PKI 是怎样管理证书和密钥的。

3. PKI 的实体构成

从广义上讲，PKI 体系是一个集网络建设、软硬件开发、信息安全技术、策略管理和相关法律政策为一体的大型的、复杂的、分布式的综合系统。一个典型、完整、有效的 PKI 系统至少应由以下部分组成：认证中心 CA、证书库（Certificate Repository，CR）、应用程序接口（Application Programming Interface，API）、密钥备份及恢复系统和证书废除系统、客户端证书处理系统。除此之外，一个 PKI 系统的运行少不了证书的申请者和证书信任方的参与。其中，认证中心、注册机构（Registration Authority，RA）和证书库 3 个部分是

PKI 的核心内容；应用程序接口则是指提供 PKI 各种基础服务的应用程序接口，使得各种应用可以与 PKI 交互，起到了桥梁和纽带作用；密钥备份及恢复系统和证书废除系统实质上是从 CA 中分离出来的功能；证书申请者和证书信任方则是利用 PKI 进行网上交易的参与者。PKI 的各个部分在具体应用中所实现的功能是有弹性的，并不是所有的功能都会出现在应用中，PKI 的许多详细功能需要根据业务的操作规程来确定。

（1）认证中心 CA

PKI 的核心是信任关系的建立和管理。直接信任和第三方信任是所有网络安全产品实现的基础。假设甲国公民 A 和乙国公民 B 互相不认识，更不信任对方，如果存在公正的可信任的第三方 C（例如护照签发机关），使 A 和 B 都直接信任 C，那么此时公民 A 和 B 就可以信任对方了，这就是所谓的第三方信任。由此可以看出在建立第三方信任时，公正、可信任的第三方 C 对于信任关系的建立和巩固起到至关重要的作用。而认证中心 CA 就扮演着这样一个具有权威性的第三方角色，是 PKI 的主要组成部分之一。其核心职责就是认证用户的身份，为信息安全提供有效的、可靠的保护机制，包括机密性、身份验证特性、不可否认性（交易的各方不可否认它们的参与）。证书机制是目前被广泛采用的一种安全机制；使用证书机制的前提是建立认证中心，以及配套的注册机构系统。

CA 是数字证书的签发机构，是 PKI 的核心，并且是 PKI 应用中权威的、可信任的、公正的第三方机构。RA 系统是 CA 证书发放、管理的延伸，具体负责证书申请者的信息录入、审核以及证书发放等工作，同时对发放的证书完成相应的管理功能；发放的数字证书可以存放于 IC 卡、硬盘或软盘等介质中；RA 系统是整个 CA 得以正常运营不可缺少的一部分。

（2）证书和证书库 CR

证书是数字证书或电子证书的简称，是构成 PKI 的基本元素。它是参与网上信息交流及商务交易活动的各个实体（例如持卡人、企业、商家和银行等）的身份证明，可证明该用户的真实身份和公钥的合法性，以及该用户与公钥的匹配关系。它相当于护照，而且是一种“电子护照”。

CR 是 CA 颁发证书和撤销证书的集中存放地，是网上的一种公共信息库，供广大公众进行开放式查询。

证书以及证书撤销信息的分发办法是发布，其思想是将 PKI 的信息放在一个广为人知的、公开且容易访问的地点，这对广大用户群体来说十分重要，因为即使属于同一群体中的人也难以互相认识。

到证书库访问查询，可以得到希望与之通信实体的公钥。若甲想与乙进行保密通信，就必须找到乙的公钥，而证书签发机构事先已将乙的身份与其公钥捆绑，进行了数字签名，发布在证书库中。甲可以通过某种可靠的、安全的方式从证书库中找到乙的证书，从而得到其公钥。

由于证书的不可伪造性，因此可以在数据库中公布，而无须其他的安全措施来保护这些证书。现在通常的做法是将证书和证书撤销信息发布到一个数据库（证书库）中，客户端可以通过多种访问协议从证书库中实时查询证书和证书撤销信息。

证书库支持分布式存放，当 PKI 所支持的环境扩充到几十万个或上百万个用户时，PKI 信息的及时和强有力的分布机制就显得非常关键，例如目录服务器的分布式存放。这是任何一个大规模的 PKI 系统成功实施的基本需求，也是创建一个有效认证机构 CA 的关键技术之一。

（3）应用程序接口 API

PKI 的价值在于使用户能够方便地使用加密、数字签名、身份认证等安全服务，因此一个完整的 PKI 必须提供良好的应用程序接口系统，使得各种各样的应用能够以安全、一致、可信的方式与 PKI 交互，确保网络环境的可信性、完整性和经济性。

（4）密钥备份及恢复系统

密钥备份及恢复是 PKI 密钥管理的重要内容之一。如果某用户由于某种原因不慎丢失了密钥，则意味着加密数据的完全丢失，那么就有可能造成合法的数据大量丢失，导致不可挽回的巨大经济损失。为了避免灾难的发生，PKI 提供了密钥备份及恢复系统。当用户证书生成的同时，解密密钥就被 CA 备份并存储起来，当需要恢复时，用户只需要向 CA 提出申请，CA 就会为用户自动进行恢复。当然，签名私钥为确保其唯一性，不能进行备份和恢复。

（5）密钥和证书的更新系统

与日常生活中我们使用的各种各样的身份证件相似，证书也有自己的使用期限，而且由于某种原因在有效期内也可能作废，例如密钥丢失、用户的个人身份信息发生改变、CA 对用户不再信任或者用户对该 CA 不再信任等各种情况。为此，证书和密钥必须要有一定的更新频率。证书的更新方式有 3 种：更换一个或多个主题的证书；更换由某一对密钥签发的所有证书；更换某一个 CA 签发的所有证书。即使在用户正常使用证书的过程中，PKI 也会自动不定时地到目录服务器中检查证书的有效期，当有效期将满时，CA 会自动启动更新程序，将旧证书列入作废证书列表（俗称黑名单），同时生成一个新证书来代替原来的证书，并通知用户。

4. PKI 的系统功能

PKI 系统由不同的功能模块组成，分别具有不同的系统功能，为了实现所提供的服务功能而有机地组成 PKI 认证体系。下面将分别介绍 PKI 体系提供的系统功能。

（1）证书申请和审批

作为以数字证书为核心实现的 PKI 安全系统，证书申请和审批功能是最基本的要求。具备证书的申请和审批功能，提供灵活、方便的申请方式，高效、可靠的审批系统，可以保证由该 PKI 体系提供安全服务的各方能顺利地得到所需要的证书。

证书的申请和审批功能直接由 CA 或面向终端用户的注册审核机构 RA 来完成。

对于行业性质的大范围 PKI 体系，证书的申请和审批一般是由 RA 来完成的。如果是通过 RA 来完成该功能，申请者需在该注册机构 RA 进行注册，申请证书。一般流程是：用户直接从 RA 处获得申请表，填写相关内容，提交给 RA，由 RA 对相关内容进行审核并决定是否通过该证书申请。通过后，RA 将申请请求及审批通过的信息提交给相应的认证中心 CA，由 CA 进行证书的签发。证书的申请和审批方式有离线和在线两种，终端用户可视

具体情况选择合适的方式。

有些简单的PKI系统中，CA和RA是一体的，即证书的申请、审批和签发一并由CA来完成。

（2）产生、验证和分发密钥

用户公/私钥对的产生、验证及分发有两种方式：用户自己产生或由代理产生。这由政策CA机构PCA的策略决定。

① 用户自己产生密钥对

用户自己选取产生密钥的方法，负责私钥的存放；用户还应该向CA提交自己的公钥和身份证明，CA对用户进行身份认证，对密钥的强度和持有者进行审核。在审核通过的情况下，对用户的公钥产生证书；然后通过面对面、信件或电子方式将证书安全地发放给用户；最后，CA负责将证书发布到相应的目录服务器。

在某些情况下，用户自己产生了密钥对后，也可到在线证书审核机构（ORA）去申请证书。此时，由ORA完成对用户的身份认证。通过后，ORA将以数字签名的方式向CA提供用户的公钥及相关信息；CA完成对公钥强度检测后产生证书，并将签名的证书返给ORA，并由ORA发放给用户或者CA通过电子方式将证书发放给用户。

② CA为用户产生密钥对

这种情况下，用户应到CA中心产生并获得密钥对。产生之后，CA中心应自动销毁本地的用户私钥备份；用户取得密钥对后，保存好自己的私钥，然后将公钥送至CA或ORA，再按照上述方式申请证书。

③ CA（包括政策批准机构PAA、政策CA机构PCA、CA）自己产生自己的密钥对

PCA的公钥证书由PAA签发，并得到PAA的公钥证书。CA的公钥由上级PCA签发，并取得上级PCA的公钥证书；当它签发下级（用户或ORA）证书时，向下级发送上级PCA及PAA的公钥证书。

（3）证书签发和下载

证书签发是PKI系统中的认证中心CA的核心功能。完成了证书的申请和审批后，将由CA签发相应证书，其中由CA所生成的证书格式应符合X.509 V3标准。

证书的发放分为离线方式和在线方式两种。

离线方式包括两个步骤：一是证书申请被批准注册后，RA端的应用程序初始化申请者的信息，在轻量级目录访问协议LDAP目录服务器中添加证书申请人的有关信息；二是RA初始化信息后传给CA，CA将相应的一次性口令和认证码通过可靠途径（电子邮件或保密信封）传递给证书申请者，证书申请者在RA处输入口令和认证码等正确信息后，在现场领取证书。证书可存入软盘或者存放于USBKey中。

在线方式包括3个步骤：一是RA端首先从CA处接收到该申请的一次性口令和认证码，然后由RA将其交给证书申请者；二是证书申请者通过Internet登录网上银行网站，通过浏览器安装根CA的证书；三是申请者在银行的网页上，按提示输入从RA处拿到的口令和认证码信息，之后就可以下载自己的证书了。

证书发放方式因各个RA的规定而有所不同，选择离线方式还是在线方式由RA视不

同的应用来决定。

（4）签名和验证

在 PKI 体系中，对信息和文件的签名，以及对数字签名的认证是很普遍的操作。

PKI 成员对数字签名和认证可以采用多种算法，例如 RSA、ECC、DES 等，这些算法可以由硬件、软件或硬软结合的加密模块（硬件）来完成。密钥和证书可以存放在内存、IC 卡、USBKey 光盘或软盘中。

（5）证书的获取

在验证信息的数字签名时，用户必须事先获取信息发送者的公钥证书，以对信息进行解密验证，同时还需要 CA 对发送者所发的证书进行验证，以确定发送者身份的有效性。证书可以通过多种方式获取：发送者发送签名信息时，附加发送自己的证书；通过单独发送证书信息的通道；可从访问发布证书的目录服务器获得；或者从证书的相关实体 RA 处获得。在 PKI 体系中，可以采取上述的某种或几种方式获得证书。

在发送数字签名证书的同时，可以发布证书链。这时，接收者拥有证书链上的每一个证书，从而可以验证发送者的证书。检验过程如下：通过检查发送者证书的发放机构 CA，从 CA 中的目录服务器取得该 CA 证书，并重复该证书链上的 CA 根证书的验证。

（6）证书和目录查询

因为证书都存在周期问题，所以进行身份验证时要保证当前证书是有效并且没过期的；另外，还有可能因密钥泄露、证书持有者身份、机构代码改变等问题，使证书需要更新。因此，在通过数字证书进行身份认证时，要保证证书的有效性。为了方便对证书有效性的验证，PKI 系统提供了对证书状态信息的查询，以及对证书撤销列表的查询机制。

CA 的目录查询通过 LDAP 协议，实时地访问证书目录和证书撤销列表，提供实时在线查询，以确认证书的状态。这种实时性要求是由金融业务或其他电子政务应用的高度敏感性和高度安全性所决定的。

（7）证书撤销

证书在使用过程中可能会因为各种原因而被废止，例如密钥泄密、相关从属信息变更、密钥有效期中止或者 CA 本身的安全隐患等。因此，证书撤销服务也必须是 PKI 的一个必需功能。该系统提供了成熟、易用、标准的证书列表作废系统，可供有关实体查询，对证书进行验证。

（8）密钥备份和恢复

密钥的备份和恢复是 PKI 中的一个重要内容。因为很多原因可能会造成丢失解密数据的密钥，那么被加密的密文将无法解开，从而造成数据丢失。为了避免这种情况的发生，PKI 提供了密钥备份与解密密钥的恢复机制，即密钥备份与恢复系统。

在 PKI 中，密钥的备份和恢复分为 CA 自身根密钥和用户密钥两种情况。

由于 CA 根密钥是整个 PKI 安全运营的基石，其安全性关系到整个 PKI 系统的安全及正常运行，因此对于根密钥的产生和备份要求很高。根密钥由硬件加密模块在加密机中产生，其备份由加密机系统管理员启动专用的管理程序执行备份过程。备份方法是将根密钥分为多块，为每一块生成一个随机口令，使用该口令加密该模块，然后将加密后的密钥块

分别写入不同的IC卡中，每个口令以一个文件形式存放，每人保存一块。恢复密钥时，由各密钥备份持有人分别插入各自保管的IC卡，并输入相应的口令才能恢复密钥。

至于用户密钥的备份和恢复，就简单多了。在CA签发用户证书时，就可以进行密钥备份。一般将用户密钥存放在CA的资料库中。进行恢复时，根据密钥对历史存档进行恢复。在完成恢复之后，相应的软件将产生一个新的签名密钥对来代替旧的签名密钥对。

（9）自动密钥更新

一个证书的有效期是有限的，这样的规定既有理论上的原因，也有实际操作上的困难。理论上有密码算法和固定密钥长度被破译的可能；实际应用中，密钥必须有一定的更换频度才能保证密钥使用的安全。但对PKI用户来说，手工完成密钥更新几乎是不可行的，因为用户经常会忽视证书已过期，只有使用失败时才能发觉。这便需要PKI系统提供密钥的自动更新功能。也就是说，无论用户的证书用于何种目的，在认证时，都会在线自动检查有效期，当失效日期到来之前的某个时间间隔内自动启动更新程序，生成一个新的证书来代替旧证书，新旧证书的序列号不同。

由于加密密钥对和签名密钥对的安全性要求不同，其密钥自动更新过程并不完全一样。对于加密密钥对和证书的更新，PKI系统采取对管理员和用户透明的方式进行，提供全面的密钥、证书及生命周期的管理。系统对快要过期的证书进行自动更新，不需要管理员和用户干预。当加密密钥对接近过期时，系统将生成新的加密密钥对。这个过程基本上与证书发放过程相同，即CA使用LDAP协议将新的加密证书发送给目录服务器，以供用户下载。

签名密钥对的更新是当系统检查证书是否过期时，对接近过期的证书，将创建新的签名密钥对。利用当前证书建立与认证中心之间的连接，认证中心将创建新的认证证书，并将证书发回RA，在归档的同时供用户在线下载。

（10）密钥历史档案

由于密钥的不断更新，经过一定的时间段，每个用户都会形成多个“旧”证书和至少一个“当前”证书。这一系列的旧证书和相应的私钥就构成了用户密钥和证书的历史档案，简称密钥历史档案。密钥历史档案也是PKI系统的一个必不可少的功能。

例如，某用户几年前加密的数据或其他人用他的公钥为其加密的数据，无法用现在的私钥解密，那么就需要从他的密钥历史档案中找到正确的解密密钥来解密数据。与此类似，有时也需要从密钥历史档案中找到合适的证书验证以前的签名。与密钥更新相同，密钥历史档案由PKI自动完成。

（11）交叉认证

交叉认证，简单地说就是把以前无关的CA连接在一起的机制，从而使得在其各自主体群之间能够进行安全通信。其实质是为了实现大范围内各个独立PKI域的互连互通、互操作而采用的一种信任模型。

交叉认证从CA所在域来分，有两种形式——域内交叉认证和域间交叉认证。域内交叉认证即进行交叉认证的两个CA属于相同的域。例如，在一个组织的CA层次结构中，某一层的一个CA认证其下一层的一个CA，这就属于域内交叉认证。域间交叉认证即两个

进行交叉认证的 CA 属于不同的域。完全独立的两个组织中的 CA 之间进行交叉认证，就是域间交叉认证。

交叉认证既可以是单向的，也可以是双向的。在一个域内，各层次 CA 体系结构中的交叉认证，只允许上一级的 CA 向下一级的 CA 签发证书，而不能相反，即只能单向签发证书。而在网状的交叉认证中，两个相互交叉认证通过“桥”——CA 互相向对方签发证书，即双向的交叉认证。

在一个行业、一个国家或者一个世界性组织等这样的大范围内建立 PKI 域，都面临着一个共同的问题，即该大范围内部的一些局部范围内可能已经建立了 PKI 域，由于业务和应用的需求，这些局部范围的 PKI 域需要进行互连互通、互操作等。为了在现有的互不连通的信息孤岛——PKI 域之间进行互通，上面介绍的交叉认证便成为合适的解决方案。

上面提到了交叉认证的实质，就是在一个确定的范围内选择合适的大范围 PKI 域信任模型（例如层次型的、网状的或桥接的等），在各个独立运行的局部 PKI 域的终端实体之间建立起信任关系，从而实现互连互通。在实现交叉认证的方案中，核心问题在于选择合适的信任模型构建大范围内合理的 CA 体系结构，根据需要建立合理的目录服务体系。其中难点在于这个大范围内的不同 PKI 域内的实体之间如何高效地建立信任路径并有效验证该信任路径。为了防止信任链的随意扩充，造成不可信的信任链，可以采取名字约束、策略约束和路径长度约束等限制措施。

（12）客户端软件

完整的 PKI 应由所需的服务器和客户端软件两部分构成。涉及到的服务器包括 CA 服务器、证书库服务器、备份和恢复服务器、时间戳服务器。所有这些功能的实现对于客户来说，还不能直接操作，需要有合理的客户端软件帮助客户实现这些系统功能。

客户端软件是一个全功能、可操作 PKI 的必要组成部分。它采取客户/服务器模型为用户提供方便的相关操作。作为提供公共服务的客户端软件应当独立于各个应用程序，提供统一、标准的对外接口，应用程序通过标准接口与客户端软件连接。如果没有客户端软件，也就无法有效地享受 PKI 提供的众多服务。

（13）时间戳服务

时间戳也叫做安全时间戳，是一个可信的时间权威，使用一段可以认证的完整数据来表示。最重要的不是时间本身的精确性，而是相关时间、日期的安全性。支持不可否认服务的一个关键因素就是在 PKI 中使用安全时间戳，也就是说，时间源是可信的，时间值必须特别安全地传送。

PKI 中必须存在用户可信任的权威时间源，权威时间源提供的时间并不需要正确，仅仅为用户提供一个参照“时间”，以便完成基于 PKI 的事务处理，例如事件 A 发生在事件 B 的前面等。一般的 PKI 系统中都设置有一个系统时钟，用以统一 PKI 的时间。当然，也可以使用世界官方时间源所提供的时间，实现方法是从网络中的权威时钟位置获得安全时间。要求实体在需要的时候向这些权威请求在数据上盖上时间戳。一份文档上的时间戳涉及到对时间和文档内容的杂凑值（哈希值）的数字签名，权威的签名提供了数据的真实性和完整性。

虽然安全时间戳是 PKI 支持的服务，但它依然可以在不依赖 PKI 的情况下实现安全时间戳服务。一个 PKI 体系中是否需要实现时间戳服务，完全视应用的需求而定。

5.3.2 PKI 的相关标准

从整个 PKI 体系建立与发展的历程来看，与 PKI 相关的标准主要包括以下几个。

1. X.209（1988）ASN.1 基本编码规则

ASN.1 是描述在网络上传输信息格式的标准方法。它有两部分：第一部分（ISO 8824/ITU X.208）描述信息内的数据、数据类型及序列格式，也就是数据的语法；第二部分（ISO 8825/ITU X.209）描述如何将各部分数据组成消息，也就是数据的基本编码规则。

ASN.1 原来是作为 X.409 的一部分而开发的，后来才独立地成为一个标准。这两个协议除了在 PKI 体系中被应用外，还被广泛应用于通信和计算机的其他领域。

2. X.500（1993）信息技术之开放系统互联标准：概念、模型及服务简述

X.500 是一套已经被国际标准化组织 ISO 接受的目录服务系统标准，它定义了一个机构如何在全局范围内共享其名称和与之相关的对象。X.500 是层次性的，其中的管理域（机构、分支、部门和工作组）可以提供相应的用户和资源信息。在 PKI 体系中，X.500 被用来唯一标识一个实体，该实体可以是机构、组织、个人或一台服务器。X.500 被认为是实现目录服务的最佳途径，但其实现需要较大的投资，并且比其他方式速度慢；而其优势是具有信息模型、多功能和开放性。

3. X.509（1993）信息技术之开放系统互联标准：鉴别框架

X.509 是由国际电信联盟 ITU-T 制定的数字证书标准。在 X.500 确保用户名称唯一性的基础上，X.509 为 X.500 用户名称提供了通信实体的鉴别机制，并规定了实体鉴别过程中广泛适用的证书语法和数据接口。

X.509 的最初版本公布于 1988 年。X.509 证书由用户公共密钥和用户标识符组成。此外，还包括版本号、证书序列号、CA 标识符、签名算法标识、签发者名称、证书有效期等信息。这一标准的最新版本是 X.509 V3，其中定义了包含扩展信息的数字证书。该版数字证书提供了一个扩展信息字段，可用来提供更多的灵活性及特殊应用环境下所需的信息传送。

4. PKCS 系列标准

PKCS 是由美国 RSA 数据安全公司及其合作伙伴制定的一组公钥密码学标准，其中包括证书申请、证书更新、证书作废表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。

5. 在线证书状态协议 OCSP

在线证书状态协议（Online Certificate Status Protocol，OCSP）是 IETF 颁布的用于检查

数字证书在某一交易时刻是否仍然有效的标准。该标准提供给 PKI 用户一条方便、快捷的数字证书状态查询通道，使 PKI 体系能够更有效、更安全地在各个领域中被广泛应用。

6. 轻量级目录访问协议 LDAP

LDAP 规范（RFC1487）简化了笨重的 X.500 目录访问协议，并且在功能性、数据表示、编码和传输方面都进行了相应的修改。1997 年，LDAP V3 成为互联网标准。目前，LDAP V3 在 PKI 体系中被广泛应用于证书信息发布、证书撤销列表 CRL 信息发布、CA 政策以及与信息发布相关的各个方面。

除了以上协议外，还有一些构建在 PKI 体系上的应用协议，这些协议是 PKI 体系在应用和普及化方面的代表作，包括 SET 协议和 SSL 协议。

目前 PKI 体系中已经包含了众多的标准和协议，由于 PKI 技术的不断进步和完善，以及其应用的不断普及，将来还会有更多的标准和协议加入。

5.4 PKI 应用举例

PKI 作为一种基础设施，其应用范围非常广泛，并且在不断发展之中，这里主要介绍当前技术领域里 PKI 技术的几个比较典型的应用实例。

1. 虚拟专用网络 VPN——PKI with IPSec

在过去几年中，VPN 越来越为企业所青睐。它是一种架构在公用通信基础设施上的专用数据通信网络，利用网络层安全协议（尤其是 IPSec）和建立在 PKI 上的加密与签名技术来获得私有性。同租用线路等方法相比，VPN 既节省开销又易于安装和使用，已经成为企业架构 Intranet 和 Extranet 的首选。

基于 PKI 技术的 IPSec 协议现在已经成为架构 VPN 的基础，它可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。虽然它的实现会复杂一些，但其安全性比其他协议都完善得多。由于 IPSec 是 IP 层上的协议，因此很容易在全世界范围内形成一种规范，具有非常好的通用性，而且 IPSec 本身就支持面向未来的协议——IPv6。总之，IPSec 还是一个发展中的协议，随着成熟的公钥密码技术越来越多地嵌入到 IPSec 中，相信在未来几年内，该协议会在 VPN 世界里扮演越来越重要的角色。

2. 安全电子邮件——PKI with S/MIME

作为 Internet 上最有效的应用，电子邮件凭借其易用、低成本和高效已经成为现代社会一种标准的信息交换工具。不过，由此引发的安全问题也日益突出。

（1）邮件和附件可以在不为通信双方所知的情况下被读取、篡改或截取。

（2）没有办法可以确定一封电子邮件是否真的来自某人，也就是说，发信者的身份可能被人伪造。

前一个问题是安全，后一个问题是信任。正是由于安全和信任的缺乏，使得公司、机构一般都不用电子邮件交换关键的商务信息，虽然电子邮件本身有着如此之多的优点。

其实，电子邮件的安全需求也是机密性、完整性、认证和不可否认性，而这些都可以利用 PKI 技术来获得。具体地说，利用数字证书和私钥，用户可以对他所发的邮件进行数字签名，这样就可以获得认证、完整性和不可否认性。如果证书是由其所属公司或某一可信第三方颁发的，收到邮件的人就可以信任该邮件的来源，无论他是否认识发邮件的人；另一方面，在政策和法律允许的情况下，用加密的方法就可以保障信息的保密性。

现实中，PGP 加密已经在电子邮件通信中得到了一定范围内的应用，这也是一种公钥加密体制，但所使用的范围比较狭窄，需要通信双方事先沟通。而基于 PKI 的安全电子邮件则具有普遍意义，因为 PKI 的用户群可以是开放的。

目前发展很快的安全电子邮件协议是 S/MIME（The Secure Multipurpose Internet Mail Extension），这是一个允许发送加密和有签名邮件的协议。该协议的实现需依赖于 PKI 技术。

3. Web 安全——PKI with SSL

浏览 Web 页面或许是人们最常用的访问 Internet 的方式。一般的浏览也许并不会让人产生不妥的感觉，可是当填写表单数据时，您有没有意识到自己的私人敏感信息可能会被一些居心叵测的人截获，而如果您或您的公司要通过 Web 进行一些商业交易，如何保证交易的安全呢？

为了透明地解决 Web 的安全问题，最合适的入手点是浏览器。现在，无论是 Internet Explorer 还是 Netscape Navigator，都支持 SSL 协议。这是一个在传输层和应用层之间的安全通信层，在两个实体进行通信之前，先要建立 SSL 连接，以此实现对应用层透明的安全通信。利用 PKI 技术，SSL 协议允许在浏览器和服务器之间进行加密通信。此外，还可以利用数字证书保证通信安全，服务器端和浏览器端分别由可信的第三方颁发数字证书，交易时双方可以通过数字证书确认对方的身份。需要注意的是，SSL 协议本身并不能提供对不可否认性的支持，这部分的工作必须由数字证书来完成。

结合 SSL 协议和数字证书，PKI 技术可以保证 Web 交易多方面的安全需求，使 Web 上的交易和面对面的交易一样安全。

4. 应用程序接口 API

协议标准是系统具有可交互性的前提和基础，它规范了 PKI 系统各部分之间相互通信的格式和步骤；而应用程序接口 API 则定义了如何使用这些协议，并为上层应用提供 PKI 服务。当应用需要使用 PKI 服务时，例如获取某一用户的公钥、请求证书废除信息或请求证书时都会用到 API。目前 API 没有统一的国际标准，大部分都是操作系统或某一公司产品的扩展，并在其产品应用的框架内提供 PKI 服务。

目前，有很多可以让开发者选择的 API 类型。IETF 建议标准为通用安全服务 API——GSS-API（Generic Security Service Application Program Interface），它提供了一种接口，与网络机制和网络协议相互独立地实现。

欧洲建立的 SESAME（Secure European System for Applications in a Multi-Vendor Environment）定义了一些安全界面，并作为该组织发展的安全技术的一部分。该接口得到了欧洲许多著名厂商的支持，如 Bull SA、ICL 和 Seimens 等，但没有在美国得到支持，特

别是一些大的厂商，如 Microsoft 和 Netscape 等。

目前在 API 市场上处于领先地位的是 Microsoft 的 CryptoAPI 和 Intel 的公用数据安全框架 CDSA（Common Data Security Architecture），它们凭借各自的产品优势相互竞争。Microsoft 主要是利用其广泛的操作系统市场，而 Intel 则凭借其 PC 芯片的优势，并与其他厂商（如 IBM、Entrust 和 Netscape 等）进行联合，共同支持 CDSA。现在也有很多厂商的 PKI 产品同时支持这两种 API，如 Entrust 等。PKIX 在很多情况下支持 CDSA，并建议其为 Architecture for Public Key Infrastructure 草案的标准。

除此之外，Entrust、IBM、Intel、Netscape 和 TIS 等联合向开放组织（Open Group）提议了一个基于 CDSA 的加密和证书管理接口，并使用了 Entrust 的 CMS API、IBM 的密钥恢复 API，但开放组织同时也在考虑使用 PKCS #11 作为安全 API 接口。

小　　结

口令机制是一种最简单、最常用的系统或应用程序访问控制的方法。因为这种认证用户的方法简单、实现容易且消耗系统资源少，至今仍在广泛地使用着。本章首先介绍了口令机制和口令所面临的安全威胁，提出了如何创建安全口令和维护口令安全的一些方法和技术。

身份鉴别技术在信息安全中处于非常重要的地位，是其他安全机制的基础，是安全系统中的第一道关卡。本章介绍了身份识别的相关概念、身份识别技术和生物身份认证技术。

口令是用于身份标识和验证的一种凭证，以密码理论为基础的身份认证和鉴别是访问控制和审计的前提，对网络环境下的信息安全尤其重要，而 PKI 为此提供了全面的解决方案。

公钥基础设施 PKI，是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务具有普遍性的安全基础设施。该体系在统一的安全认证标准和规范基础上提供了在线身份认证，是 CA 认证、数字证书、数字签名以及相关的安全应用组件的集合。

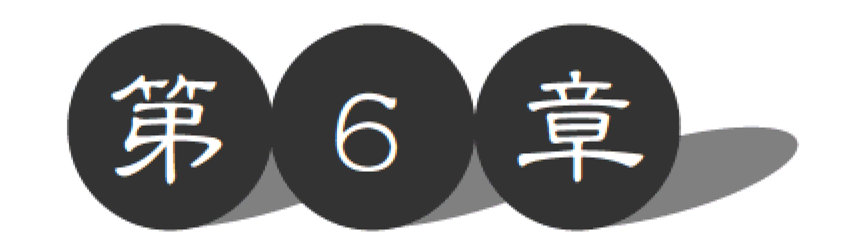
PKI 的核心是解决信息网络空间中的信任问题，确定信息网络、信息空间中各种经济、军事和管理行为的主体（包括组织和个人）身份的唯一性、真实性和合法性，为组织机构建立和维护一个可信赖的系统环境，透明地为应用系统提供身份认证、数据保密性和完整性、抗抵赖等各种必要的安全保障，满足各种应用系统的安全需求。

PKI 作为一种基础设施，其应用范围非常广泛，这里介绍了在虚拟专用网络 VPN、安全电子邮件、Web 安全、应用程序接口 API 等方面的应用。

练习与思考

1. 口令面临的安全威胁有哪些方面？
2. 维护口令的安全应从哪些方面进行？

3. 什么是身份识别？身份识别技术有哪些？
4. 身份鉴别可利用的生物特征必须满足怎样的条件？
5. 什么是 PKI？它有哪些服务功能？
6. PKI 实体由哪几部分构成？各部分主要完成什么功能？
7. 什么是 CA？它的功能是什么？
8. 什么是数字证书？什么是时间戳服务？
9. 什么是 KMC？它主要完成什么功能？



防火墙工作原理及应用

本章学习要求：

（1）了解防火墙的基本概念、发展简史、目的、功能、局限性及其发展动态和趋势。

（2）了解防火墙的不同分类方法。

（3）掌握包过滤技术的基本原理、技术特点和实现方式，了解包过滤技术的优、缺点。

（4）掌握代理服务技术、应用层网关防火墙和电路级网关防火墙的基本原理、技术特点和实现方式，了解代理服务技术的优、缺点。

（5）了解状态检测技术和自适应代理技术的基本原理和技术特点。

（6）掌握屏蔽路由器体系结构、双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构等 4 种防火墙体系结构的基本组成。

（7）了解多种组合体系结构的基本组成。

（8）熟悉防火墙的产品选购和设计策略。

（9）了解个人版防火墙的特点，了解瑞星个人版防火墙的操作方法。

重点和难点：

（1）重点：包过滤技术；代理服务技术；应用层网关防火墙和电路级网关防火墙；状态检测技术和自适应代理技术的基本原理、技术特点和实现方式；屏蔽路由器体系结构、双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构等 4 种防火墙体系结构的基本组成。

（2）难点：多种组合体系结构的基本组成。

随着互联网的发展和网络应用的不断深入，来自网络外部和内部的安全威胁不断涌现，给网络的管理者和使用者带来了极大的困扰。防火墙的出现，在一定程序上满足了人们对网络安全的要求。

众所周知，防火墙（Firewall）是一种将内部网和公用网（例如 Internet）分开的方法，可对被保护的网络与 Internet 网络之间，或者与其他网络之间进行的信息存取和传递操作等

进行控制。防火墙可以作为不同网络或网络安全域之间信息的出入口，能根据一个单位的安全策略控制出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础设施。在逻辑上，防火墙是一个分离器、一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的所有活动，保证了内部网络的安全。

从本质上讲，防火墙是一种访问控制系统，除了可以用来保护与互联网相连的内部网外，还可以用于保护其他网络对象，例如子网或主机。

在构建安全网络环境的过程中，防火墙作为第一道安全防线，正受到越来越多用户的关注。通常一个单位在购买网络安全设备时，总是把防火墙放在首位。目前，防火墙已经成为世界上用得最多的网络安全产品之一。本章的主要目的就是讲述防火墙是如何保证网络系统安全的。

6.1 防火墙概述

6.1.1 防火墙的基本概念

防火墙的最初目的，是为了防止火和热的蔓延。以前的火车都是用蒸汽机提供动力的，在火车头里面有一个烧水的锅炉，需要机师向里面不断地添煤，才能保证有持续的能量供给。但是当时的技术不能保证蒸汽机的稳定性能，经常出现爆炸事件。一旦爆炸，火车头里的机师肯定会有生命危险，而且火势也会蔓延到其他车厢，造成乘客的伤亡。

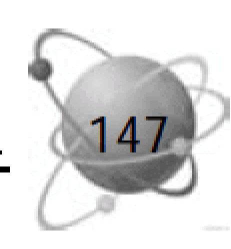
为了保护车厢内乘客的安全，有人想出了一种办法——在车头和车厢之间用钢板隔断，这样可以在蒸汽机发生爆炸的时候，防止火势蔓延，从而保证乘客的安全。这就是最初的防火墙。

从这里可以看出防火墙的基本功能：它是一个位于内部和外部之间的安全屏障，可以防止外部的某种威胁。但是防火墙不能防止来源于内部的威胁——如果蒸汽机发生爆炸，内部的机师肯定还会遇难。

在今天的信息世界里，人们借助了这个概念，使用防火墙来保护敏感的数据不被窃取和篡改，不过这些防火墙是由先进的计算机硬件或软件系统构成的。

防火墙通常是指设置在不同网络（例如可信任的内部网络和不可信任的外部网络）或网络安全域之间的一系列部件的组合。它是一种必不可少的安全增长点，是设置在被保护网络和外部网络之间的一道屏障，也是不同网络或网络安全域之间信息的唯一出入口，能根据网络安全策略控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础和核心控制设备，能够有效地监控内部网和互联网之间的任何活动，防止发生不可预测的、潜在破坏性的侵入，从而保证内部网络的安全。

防火墙示意图如图 6-1 所示。



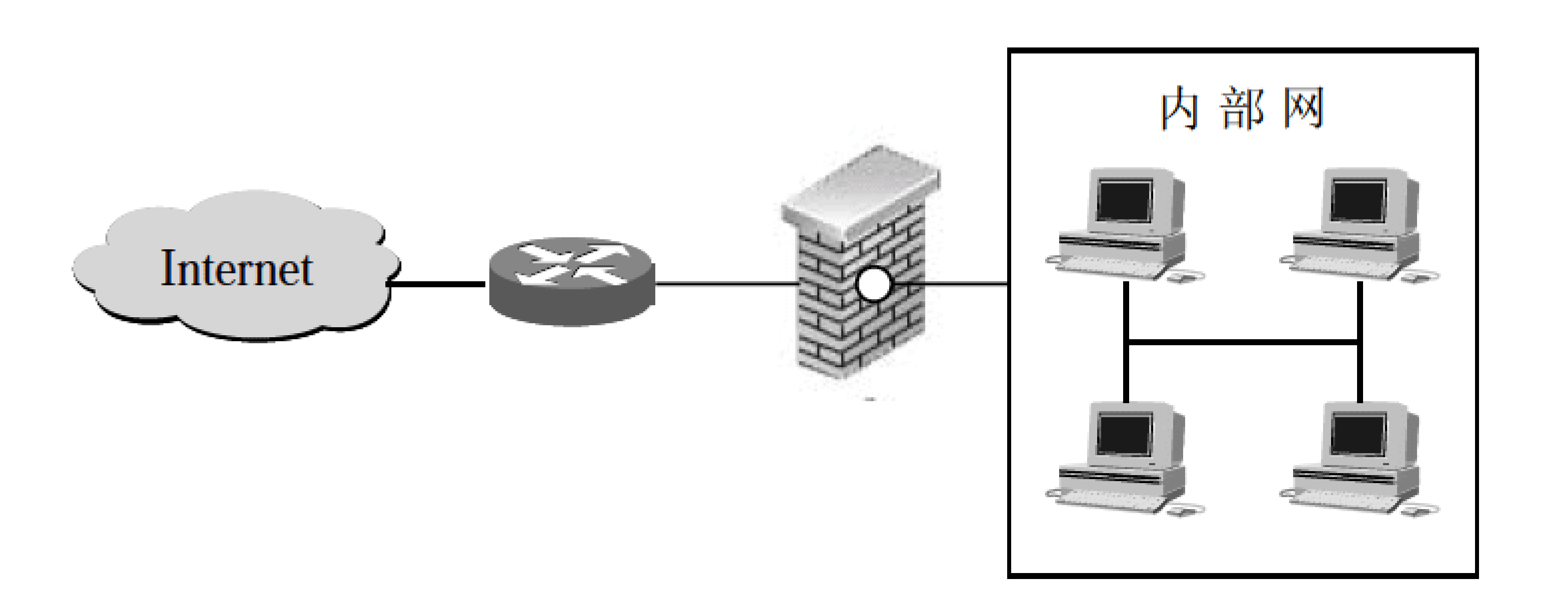


图 6-1　网络防火墙

防火墙作为网络安全的第一道防线，概括地说，一般具有以下 5 项基本功能。

（1）过滤进出网络的数据。

（2）管理进出网络的访问行为。

（3）封堵某些禁止的业务。

（4）记录通过防火墙的信息内容和活动。

（5）对网络攻击进行检测和报警。

6.1.2　防火墙的发展简史

第一代防火墙：1983 年，第一代防火墙几乎与路由器同时出现，采用了包过滤（Packet Filter）技术。

第二代防火墙：1989 年，贝尔实验室的 Dave.Presotto 和 Howard.Trickey 推出了第二代防火墙，即电路级防火墙，同时提出了应用层防火墙（代理防火墙）的初步结构。

第三代防火墙：1992 年，USC 信息科学学院的 Bob.Braden 开发出了基于动态包过滤（Dynamic Packet Filter，DPF）技术的第三代防火墙，后来演变为目前所说的状态监视（State Fulinspection，SF）技术。1994 年，以色列的 Check.Point 公司开发出了第一个基于这种技术的商业化产品。

第四代防火墙：防火墙技术和产品随着网络攻击和安全防护手段的发展而演进，到 1997 年初，具有安全操作系统的防火墙产品面世，使防火墙技术步入了第四代。具有安全操作系统的防火墙本身就是一个操作系统，因而在安全性上较之以前的防火墙有了质的提高。

第五代防火墙：1998 年，NAI 公司推出了一种自适应代理（Adaptive Proxy，AP）技术，并在其产品 Gauntlet Firewall for NT 中得以实现，给代理类型的防火墙赋予了全新的意义，可以称之为第五代防火墙。

6.1.3　设置防火墙的目的和功能

在没有防火墙时，局域网内部的每个节点都暴露给 Internet 上的其他主机，此时内部网的安全性要由每个节点的坚固程度来决定，且安全性等同于其中最薄弱的节点。使用防火墙后，防火墙会将内部网的安全性统一到它自身，网络安全性在防火墙系统上得到加固，而不是分布在内部网的所有节点上。防火墙把内部网与 Internet 隔离，仅让安全、核准了的

信息进入，而阻止对内部网构成威胁的数据，这样即可防止黑客更改、复制、毁坏重要信息，同时又不会妨碍人们对 Internet 的访问。

具体地说，通常应用防火墙的目的有以下几个方面：限制他人进入内部网络；过滤掉不安全的服务和非法用户；防止入侵者接近用户的防御设施；限定人们访问特殊站点；为监视局域网安全提供方便。

防火墙的主要功能就是控制对受保护网络的非法访问，它通过监视、限制、更改通过网络的数据流，一方面尽可能屏蔽内部网的拓扑结构，另一方面对内屏蔽外部危险站点，用以防范外对内、内对外的非法访问。

防火墙的工作原理如图 6-2 所示。

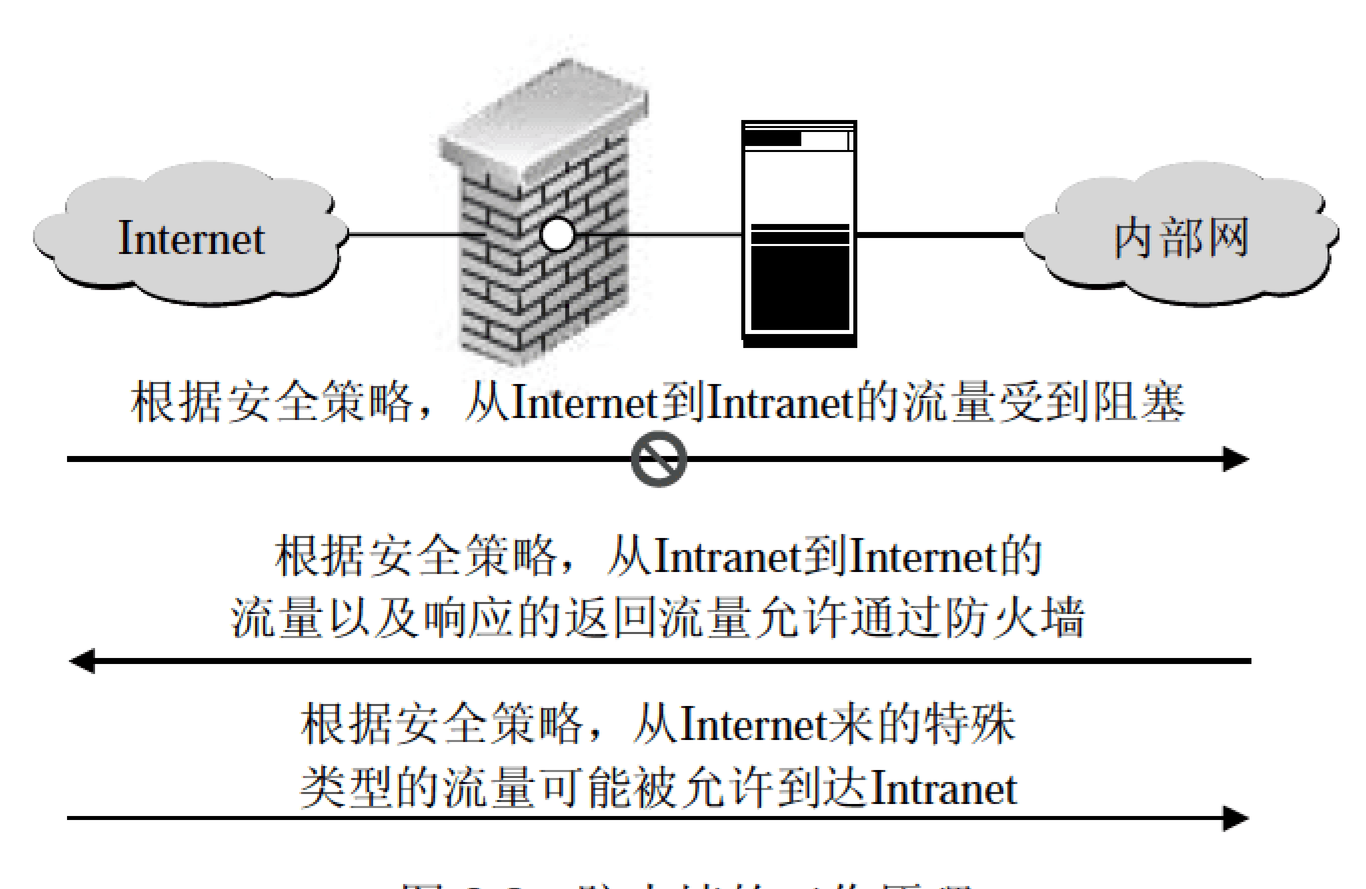


图 6-2 防火墙的工作原理

防火墙的功能主要表现在以下 4 个方面：

（1）防火墙是网络安全的屏障

防火墙作为一个阻塞点、控制点，能极大地提高内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议数据包才能通过防火墙，所以使内部网络环境变得更安全。例如，防火墙可以禁止诸如众所周知的不安全的 NFS 协议数据包进出受保护的网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。同时防火墙可以保护网络免受基于路由的攻击，例如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路由攻击。防火墙应该可以拒绝所有以上类型攻击的报文，并通知防火墙管理员。

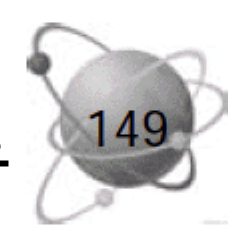
（2）防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，可将所有安全技术，例如口令、加密、身份认证、审计等配置在防火墙上。

与将网络安全问题分散到各个主机上相比，选择防火墙的集中安全管理更经济。

（3）对网络存取和访问进行监控审计

如果所有的访问都经过防火墙，那么防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。



另外，收集一个网络的使用和误用情况也是非常重要的：它可以使防火墙管理员清楚地了解到防火墙是否能够抵挡攻击者的探测和攻击、防火墙的控制是否充足等；网络的使用统计对网络需求分析和威胁分析等而言，也是非常重要的。

（4）防止内部信息的外泄

利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。

隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些可能被透漏的内部细节，例如 Finger、DNS 等服务。Finger 显示了主机上所有用户的注册名、真名、最后登录的时间和使用的 Shell 类型等，这些信息非常容易被攻击者获悉。攻击者可以利用这些信息知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样内部主机的域名和 IP 地址就不会被外界所了解。

除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，企事业单位在地域上分布在全世界各地的 LAN 或专用子网即可有机地联成一个整体，不仅省去了专用通信线路，而且为信息共享提供了技术保障。

总之，防火墙允许网络管理员定义一个核心点来防止非法用户进入内部网络；可以很方便地监视网络的安全性，并报警；可以作为部署网络地址变换（Network Address Translation，NAT）的地点，利用 NAT 技术，将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来，用来缓解地址空间短缺的问题；防火墙还是审计和记录 Internet 使用费用的一个最佳地点，网络管理员可以在此向管理部门提供 Internet 连接的费用情况，查出潜在的带宽瓶颈位置，并可依据本机构的核算模式提供部门级的计费；防火墙可以连接到一个单独的网段上（从技术角度来讲，这就是所谓的停火区——DMZ），从物理上和内部网段隔开，并在此部署 WWW 服务器和 FTP 服务器，将其作为向外部发布内部信息的地点。

6.1.4　防火墙的局限性

防火墙技术是内部网络最重要的安全技术之一，得到了高度关注和广泛应用。不过，也由此产生了一个误解，即防火墙是万能的。目前防火墙产品集成的功能越来越多，人们对它的期望也很高，甚至有人认为有了防火墙就有了安全保障。事实上，安装防火墙并不能做到绝对的安全，尚有许多防范不到的地方。具体如下：

（1）防火墙不能防范不经由防火墙的攻击

防火墙可以有效地检查经由它进行传输的信息，但不能防止绕过它进行传输的信息。例如，如果允许从受保护网络的内部不受限制地向外拨号，一些用户便可形成与 Internet 的直接连接，从而绕过防火墙，造成一个潜在的攻击渠道。

（2）防火墙不能防止感染了病毒的软件或文件的传输

如今恶意程序发展迅速，病毒可依附于共享文档进行传播，也可通过 E-mail 附件的形

式在 Internet 上迅速蔓延。Web 本身就是一个病毒源，许多站点都可以下载病毒程序甚至源码。另外，病毒的类型、隐藏和传输方式太多，操作系统也有多种，不能期望防火墙去对每一个进出内部网络的文件进行扫描，查出潜在的病毒；否则，防火墙将成为网络中最大的瓶颈。

（3）防火墙不能防止数据驱动型攻击

有些表面看起来无害的数据通过电子邮件发送或者其他方式复制到内部主机上，一旦被执行就形成攻击。一个数据驱动型攻击，可能导致主机修改与安全相关的文件，使得入侵者很容易获得对系统的访问权。

（4）防火墙不能防范恶意的内部人员入侵

一般来说，防火墙的安全控制只能作用于外对内或内对外，即对外可屏蔽内部网的拓扑结构，封锁外部网上的用户连接到内部网上的重要站点或某些端口：对内可屏蔽外部危险站点，但它并不能控制内部用户对内部网络的越权访问。内部人员通晓内部网络的结构，如果他从内部入侵内部主机，或进行一些破坏活动，例如窃取数据、破坏硬件和软件，因为该通信没有通过防火墙，防火墙也就无法阻止。

所以说，内部用户攻击网络正是网络安全最大的威胁。据权威部门统计表明，网络上的安全攻击事件有 70%以上来自内部。也就是说，防火墙基本上是防外不防内。

（5）防火墙不能防范不断更新的攻击方式

由于防火墙的安全策略是在已知的攻击模式下制定的，只能防御已知的威胁，对于全新的攻击方式缺少阻止功能。

（6）防火墙难于管理和配置，易造成安全漏洞

防火墙的管理及配置相当复杂，要想成功地维护防火墙，防火墙管理员对网络安全攻击的手段及其与系统配置的关系必须有着相当深刻的了解。

防火墙的安全策略无法进行集中管理，一般来说，由多个系统（路由器、过滤器、代理服务器、网关、堡垒主机）组成的防火墙，管理上有所疏忽是在所难免的。

（7）很难为用户在防火墙内外提供一致的安全策略

许多防火墙对用户的安全控制主要是基于用户所用机器的 IP 地址而不是用户身份，这样就很难为同一用户在防火墙内外提供一致的安全控制策略，限制了网络的物理范围。

总之，一方面，防火墙在当今 Internet 世界中的存在是有生命力的；另一方面，防火墙不能替代内部谨慎的安全措施。因此，它不是解决所有网络安全问题的万能药方，而只是网络安全策略中的一个组成部分。

6.1.5 防火墙技术的发展动态和趋势

考虑到 Internet 发展的迅猛势头和防火墙产品的更新步伐，要全面展望防火墙技术的发展几乎是不可能的。但是，从产品及功能上，却又可以看出一些动态和趋势。

防火墙产品正向以下趋势发展：

1. 优良的性能

新一代防火墙系统不仅应该能更好地保护防火墙后面内部网络的安全，而且应该具有更为优良的整体性能。

传统的代理型防火墙虽然可以提供较高级别的安全保护，但是同时它也成为限制网络带宽的瓶颈，这极大地制约了它在网络中的实际应用。

现在大多数的防火墙产品都支持 NAT 功能，它可以让受防火墙保护的内部网络的 IP 地址不至于暴露给外部网络；但启用 NAT 后，势必会对防火墙的系统性能有所影响，如何尽量减少这种影响也成为目前防火墙产品的卖点之一。

另外，防火墙系统中集成的 VPN 解决方案必须是真正的线速运行，否则将成为网络通信的瓶颈。特别是采用复杂的加密算法时，防火墙性能尤为重要。总之，未来的防火墙系统将会把高速的性能和最大限度的安全性有机结合在一起，有效地消除制约传统防火墙的性能瓶颈。

2. 可扩展的结构和功能

选择哪种防火墙，除了应考虑其基本性能外，毫无疑问，还应考虑用户的实际需求与未来网络的升级。因此，防火墙除了具有保护网络安全的基本功能外，还应提供对 VPN 的支持，同时还应该具有可扩展的内驻应用层代理。除了支持常见的网络服务以外，还应该能够按照用户的需求提供相应的代理服务。例如，如果用户需要 X-Window、HTTP 和 Gopher 等服务，防火墙就应该包含相应的代理服务程序。

未来的防火墙系统应是一个可随意伸缩的模块化解决方案，从最基本的包过滤到带加密功能的 VPN 型包过滤，直至一个独立的应用网关，使用户有充分的余地构建自己所需要的防火墙体系。

3. 简化的安装与管理

防火墙产品配置和管理的难易程度，是防火墙能否达到目的的主要考虑因素之一。若防火墙的配置和管理过于困难，则可能会造成设定上的错误，反而不能达到其功能。

未来的防火墙将具有非常易于进行配置的图形用户界面，NT 防火墙市场的发展充分证明了这种趋势。

4. 主动过滤

许多防火墙都包括对过滤产品的支持，并可以与第三方过滤服务连接，这些服务提供了不受欢迎的 Internet 站点的分类清单。

防火墙还在它们的 Web 代理中包括了时间限制功能，允许非工作时间的冲浪和登录，并提供冲浪活动的报告。

5. 防病毒与防黑客

许多防火墙具有内置防病毒与防黑客的功能。

防火墙技术下一步的走向和选择，也可能会包含以下几个方面。

（1）防火墙将从目前对子网或内部网络管理的方式向远程上网集中管理的方式发展。

（2）过滤深度不断加强，从目前的地址、服务过滤，发展到 URL（页面）过滤、关键字过滤和对 ActiveX、Java 小应用程序等的过滤，并逐渐有病毒清除功能。

（3）利用防火墙建立专用网 VPN 是较长一段时间的主流，IP 的加密需求越来越强，安全协议的开发是一大热点。

（4）对网络攻击的检测和报警将成为防火墙的重要功能。

（5）安全管理工具不断完善，特别是可疑活动的日志分析工具等将成为防火墙产品中的一部分。

综上所述，未来防火墙技术会全面考虑网络的安全、操作系统的安全、应用程序的安全、用户的安全、数据的安全等 5 个方面。此外，防火墙产品还将把网络前沿技术，如 Web 页面超高速缓存、虚拟网络和带宽管理等与其自身结合起来。

6.2 防火墙技术

6.2.1 防火墙的分类

防火墙有多种不同的分类方法：根据采用的技术不同，可分为包过滤防火墙和代理服务器防火墙；按照应用对象的不同，可分为企业级防火墙与个人防火墙；依据实现的方法不同，又可分为软件防火墙、硬件防火墙和专用防火墙。

1. 基于实现方法分类

软件防火墙运行于作为网关的特定计算机上，需要先在计算机上安装并做好配置才可以使用。使用这类防火墙，需要网络管理人员对所工作的操作系统平台比较熟悉。

硬件防火墙是在定制的 PC 硬件上，运行经过最小化安全处理后的通用操作系统及集成的防火墙软件。其特点是开发成本低、性能实用、稳定性和扩展性较好，价格也低廉。由于此类防火墙依赖操作系统内核，因此会受到操作系统本身的安全性影响，处理速度也比较慢。

专用防火墙采用特别优化设计的硬件体系结构，使用专用的操作系统。此类防火墙在稳定性和传输性能方面有着得天独厚的优势，速度快，处理能力强，性能高，并且系列化程度高；由于使用专用操作系统，容易配置和管理，本身漏洞也比较少；但是扩展能力有限，价格也比较高。

2. 基于防火墙技术原理分类

互联网采用 TCP/IP 协议，在不同的网络层次上设置不同的屏障，构成不同类型的防火墙。因此，从工作原理角度看，防火墙技术主要可分为网络层防火墙技术和应用层防火墙技术。这两个层次的防火墙技术的具体实现有包过滤防火墙、代理服务器防火墙、状态检测防火墙和自适应代理防火墙等。

3. 基于防火墙硬件环境分类

根据实现防火墙的硬件环境不同，可将防火墙分为基于路由器的防火墙和基于主机系统的防火墙。包过滤防火墙和状态检测防火墙可以基于路由器，也可基于主机系统实现；而代理服务器防火墙只能基于主机系统实现。

4. 基于防火墙的功能分类

根据防火墙的功能不同，可将防火墙分为 FTP 防火墙、Telnet 防火墙、E-mail 防火墙、病毒防火墙、个人防火墙等各种专用防火墙。通常也将几种防火墙技术组合在一起使用，以弥补各自的缺陷，增加系统的安全性能。

6.2.2 包过滤技术

1. 基本原理

包过滤（Packet Filtering，PF）是防火墙为系统提供安全保障的主要技术，可在网络层对进出网络的数据包进行有选择的控制与操作。包过滤操作一般都是在选择路由的同时，在网络层对数据包进行选择或过滤。

选择的依据是系统内设置的过滤逻辑，即访问控制表（Access Control Table，ACT）。由它指定允许哪些类型的数据包可以流入或流出内部网络。例如，如果防火墙中设定某一 IP 地址的站点为不适宜访问的站点，则从该站点地址来的所有信息都会被防火墙过滤掉。一般过滤规则是以 IP 数据包信息为基础，对 IP 数据包的源地址、目的地址、传输方向、分包、IP 数据包封装协议（例如，TCP/UDP/ICMP）、TCP/UDP 目标端口号等进行筛选、过滤。

包过滤技术是一种网络安全保护机制，可以用来控制流出和流入网络的数据。它有选择地让数据包在内部网络与外部网络之间进行交换，即根据内部网络的安全规则允许某些数据包通过，同时又阻止某些数据包通过。它通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合，决定该 IP 数据包是否要进行拦截还是给予放行。这样可以有效地防止恶意用户利用不安全的服务对内部网进行攻击。

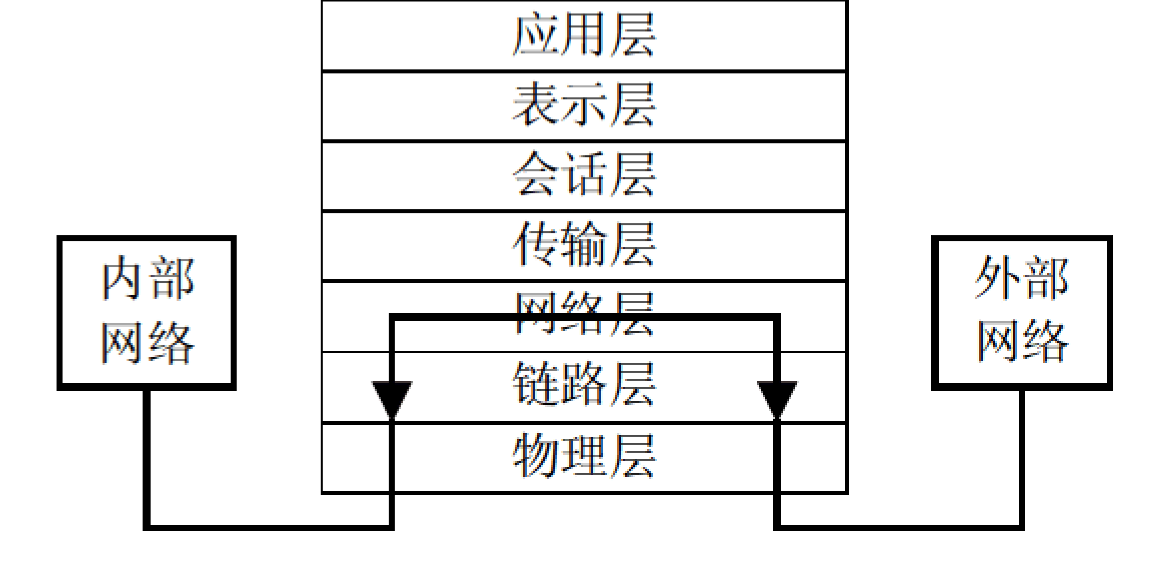


图 6-3　包过滤防火墙工作原理

包过滤防火墙的工作原理如图 6-3 所示。

包过滤防火墙要遵循的一条基本原则就是“最小特权原则”，即明确允许管理员希望通过的那些数据包，禁止其他的数据包。

2. 包过滤技术的优点

包过滤防火墙逻辑简单，价格低廉，易于安装和使用，网络性能和透明性好。它通常

安装在路由器上，而路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

包过滤防火墙的优点主要体现在下面几个方面：

（1）不用改动应用程序

包过滤防火墙不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。

（2）一个过滤路由器能协助保护整个网络

包过滤防火墙的主要优点之一，是一个单个的、恰当放置的包过滤路由器有助于保护整个网络。如果仅有一个路由器连接内部与外部网络，则不论内部网络的大小、内部拓扑结构如何，通过那个路由器进行数据包过滤，在网络安全保护上就能取得较好的效果。

（3）数据包过滤对用户透明

数据包过滤是在 IP 层实现的，Internet 用户根本感觉不到它的存在；包过滤不要求任何自定义软件或者客户机配置；它也不要求用户经过任何特殊的训练或者操作，使用起来很方便。

较强的“透明度”是包过滤的一大优势。

（4）过滤路由器速度快、效率高

过滤路由器只检查报头相应的字段，一般不查看数据包的内容，而且某些核心部分是由专用硬件实现的，故其转发速度快、效率较高。

总之，包过滤技术是一种通用、廉价、有效的安全手段。通用，是因为它不针对各个具体的网络服务采取特殊的处理方式，而是对各种网络服务都通用；廉价，是因为大多数路由器都提供分组过滤功能，不用再增加更多的硬件和软件；有效，是因为它能在很大程度上满足企业的安全要求。

3．包过滤的缺点

（1）安全性较差

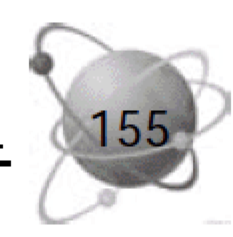
过滤判别的只有网络层和传输层的有限信息，因而各种安全要求不可能得到充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响；由于缺少上下文关联信息，不能有效地过滤诸如 UDP、RPC 一类的协议；非法访问一旦突破防火墙，即可对主机上的软件和配置漏洞进行攻击；大多数过滤路由器中缺少审计和报警机制，通常没有用户的使用记录，这样管理员就不能从访问记录中发现黑客的攻击记录，而攻击一个单纯的包过滤式的防火墙对黑客来说是比较容易的，因为他们在这一方面已经积累了大量的经验。

（2）一些应用协议不适用

对于一些应用协议，如 RPC、X-Window 和 FTP 等不适用。

（3）正常的数据包过滤路由器无法执行某些安全策略

数据包过滤路由器上的信息不能完全满足用户对安全策略的需求。例如，数据包的报头信息只能说明数据包来自什么主机，而不是什么用户；数据包到什么端口，而不是到什



么应用程序。这就存在着很大的安全隐患和管理控制漏洞。

（4）不能彻底防止地址欺骗

大多数包过滤路由器都是基于源 IP 地址、目的 IP 地址而进行过滤的，而数据包的源地址、目的地址以及 IP 的端口号都在数据包的头部，很有可能被窃听或假冒（IP 地址的伪造是很容易、很普遍的）。如果攻击者把自己主机的 IP 地址设成一个合法主机的 IP 地址，就可以很轻易地通过报文过滤器。所以，包过滤防火墙最主要的弱点是不能在用户级别上进行过滤，即不能识别不同的用户和防止 IP 地址的盗用。

过滤路由器在这点上大都无能为力。即使按 MAC 地址进行绑定，也是不可信的。对于一些安全性要求较高的网络，过滤路由器是不能胜任的。

（5）数据包工具存在很多局限性

例如，数据包过滤规则难以配置，管理方式和用户界面较差；对安全管理人员素质要求比较高；建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。

从以上分析可以看出，包过滤防火墙技术虽然能起到一定的安全保护作用，且也有许多优点，但它毕竟是第一代防火墙技术，本身存在较多缺陷，不能提供较高的安全性。因此，在实际应用中，很少把包过滤技术当作单独的安全解决方案，通常是把它与应用网关配合使用或与其他防火墙技术揉合在一起使用，共同组成防火墙系统。

6.2.3　代理服务技术

随着包过滤防火墙缺点的不断显现，许多安全专家开始寻找更好的防火墙安全机制。他们相信真正可靠的安全防火墙应该禁止所有通过防火墙的直接连接——在协议栈的最高层检验所有的输入数据。为测试这一理论，DARPA（Defense Advanced Research Projects Agency）和在华盛顿享有较高声望的以可信信息系统著称的高级安全研究机构签订了合同，着手开发安全的“应用级代理”防火墙。这一研究最终造就了 Gauntlet（http://www.tis.com/）——第一代以 DARPA 和美国国防部的最高标准设计的商业化应用级代理防火墙的诞生。应用级代理防火墙模式提供了十分先进的安全控制机制，它通过在协议栈的最高层（应用层）检查每一个包来提供足够的应用级连接信息。因为在应用层中具有足够的能见度，应用级代理防火墙很容易就能看见前面提及的每一个连接的细节，从而实现各种安全策略。例如，这种防火墙很容易识别重要的应用程序命令，像 FTP 的上传请求 put 和下载请求 get。

代理防火墙工作于应用层，且针对特定的应用层协议，通过代理可以实现比包过滤更严格的安全策略。

代理（Proxy）防火墙分为应用层网关和电路级网关两类。

1．基本原理

代理服务器是运行在防火墙主机上的一些特定的应用程序或者服务程序，它们代表客户在服务器端进行连接请求。当代理服务器收到一个客户的连接请求时，它将核实客户请

求，并用特定的安全化的代理应用程序来处理连接请求，并将处理后的请求传递到真实的服务器上，然后接收服务器应答，并作进一步处理后，将答复交给发出请求的最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接和隔离内、外部网络的作用，所以又称为代理防火墙。

代理防火墙的应用层代理服务的数据控制及传输过程如图 6-4 所示。

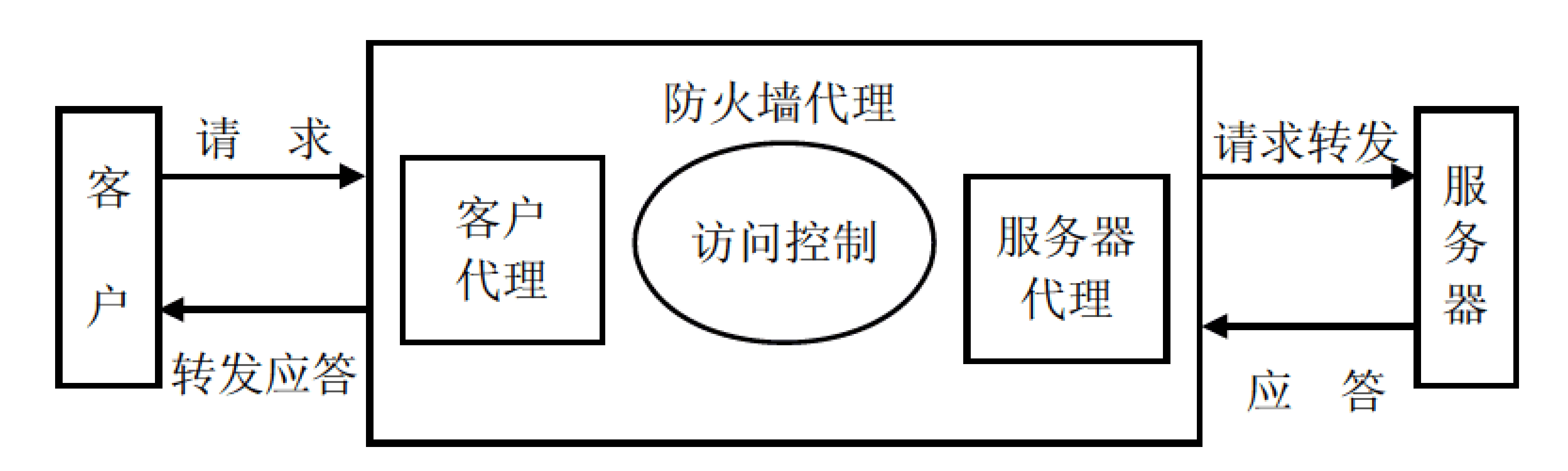


图 6-4 代理防火墙的应用层数据控制及传输过程

代理防火墙最突出的特点是，将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”，由两个代理服务器上的“链接”来实现，外部计算机的网络链路只能到达代理服务器，从而起到隔离防火墙内外计算机系统的作用。此外，代理防火墙在发现被攻击的迹象时，将向网络管理员发出警报，并保留攻击现场。也就是说，在代理服务中，内部各站点之间的连接被切断了，代理服务在幕后操纵着各站点间的连接。

2. 应用层网关防火墙

（1）工作原理

应用层网关（Application Level Gateways，ALG）防火墙是传统代理型防火墙，在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时对数据包进行必要的分析、登记和统计，形成报告。

应用层网关防火墙的工作原理如图 6-5 所示。

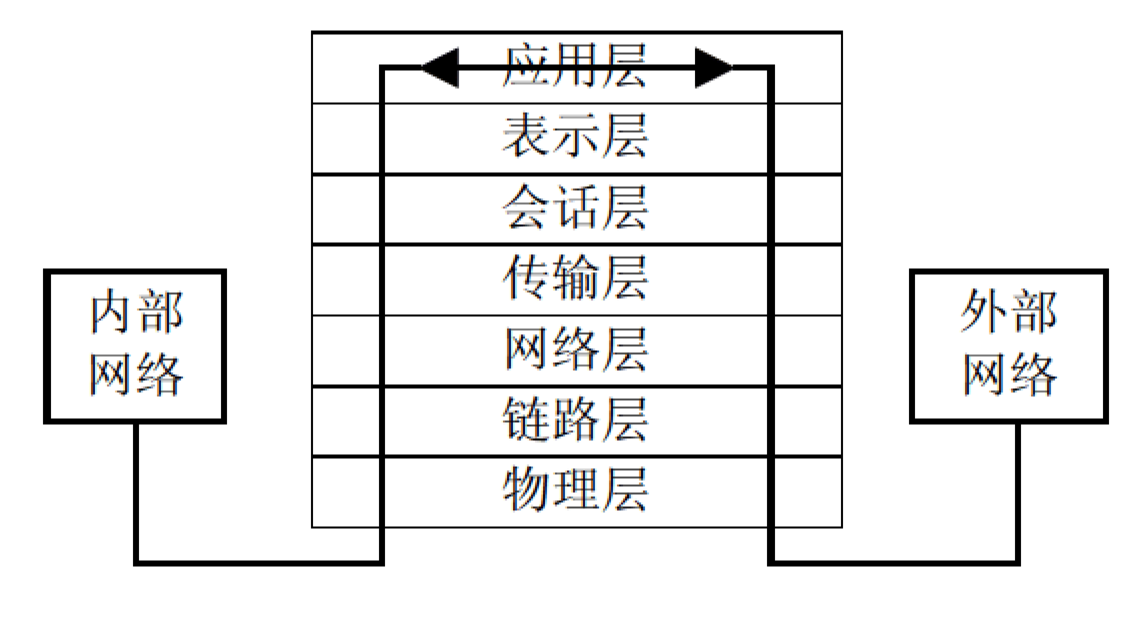


图 6-5 应用网关防火墙实现原理

应用层网关防火墙的核心技术就是代理服务器技术，它是基于软件的，通常安装在专用工作站系统上。这种防火墙通过代理技术参与到一个 TCP 连接的全过程，并在网络应用层上建立协议过滤和转发功能，所以叫做应用层网关。当某用户（不管是远程的还是本地的）想和一个运行代理的网络建立联系时，此代理（应用层网关）会阻塞这个连接，然后在过滤的同时对数据包进行必要的分析、登记和统计，形成检查报告。如果此连接请求符



合预定的安全策略或规则，代理防火墙便会在用户和服务器之间建立一个“桥”，从而保证其通信。对不符合预定安全规则的，则阻塞或抛弃。换句话说，“桥”上设置了很多控制。

同时，应用层网关将内部用户的请求确认后送到外部服务器，再将外部服务器的响应回送给用户。这种技术对 ISP 很常见，通常用于在 Web 服务器上高速缓存信息，并且扮演 Web 客户和 Web 服务器之间的中介角色。它主要保存 Internet 上那些最常用和最近访问过的内容：在 Web 上，代理首先试图在本地寻找数据；如果没有，再到远程服务器上去查找。为用户提供了更快的访问速度，并且提高了网络的安全性。

（2）优点

应用层网关防火墙最突出的优点就是安全，这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。由于每一个内外网络之间的连接都要通过代理的介入和转换，通过专门为特定的服务（例如 HTTP）编写的安全化的应用程序进行处理，然后由防火墙本身提交请求和应答，没有给内外网络的计算机以任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网络。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用；而包过滤类型的防火墙是很难彻底避免这一漏洞的。

应用层网关防火墙同时也是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用，它工作在 OSI 模型的最高层，掌握着应用系统中可用作安全决策的全部信息。

（3）缺点

代理防火墙的最大缺点就是速度相对比较慢，当用户对内外网络网关的吞吐量要求比较高时，例如要求达到 75～100Mbps 时，代理防火墙就会成为内外网络之间的瓶颈。所幸的是，目前用户接入 Internet 的速度一般都远低于这个数字。在现实环境中，也要考虑使用包过滤类型防火墙来满足速度要求的情况，大部分是高速网（ATM 或千兆位 Intranet 等）之间的防火墙。

3. 电路级网关防火墙

另一种类型的代理技术称为电路级网关（Circuit Level Gateway，CLG）或 TCP 通道（TCP Tunnels）防火墙。在电路级网关防火墙中，数据包被提交给用户的应用层进行处理，电路级网关用来在两个通信的终点之间转换数据包，如图 6-6 所示。

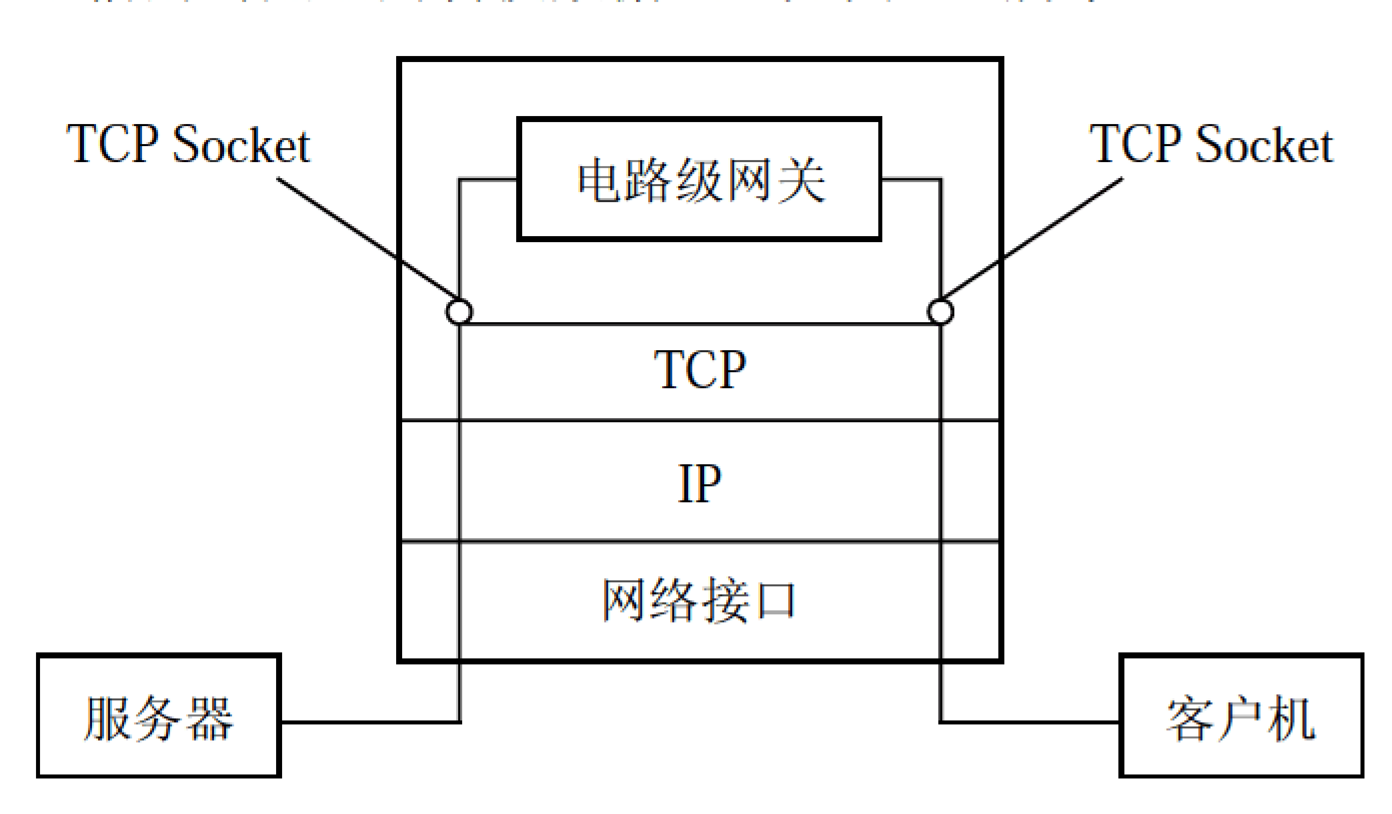


图 6-6 电路级网关防火墙

电路级网关是建立应用层网关的一种更加灵活的方法，是针对包过滤和应用层网关技术存在的缺点而引入的防火墙技术。电路级网关通过在 TCP 3 次握手建立连接的过程中，检查双方的 SYN、ASK 和序列号是否符合逻辑，来判断该请求的会话是否合法。一旦网关认为会话是合法的，就为双方建立连接，并维护一张合法会话连接表，当会话信息与表中的条目匹配时才允许数据通过，会话结束后，表中的条目就被删除。

电路级网关防火墙与包过滤防火墙都是依靠特定的逻辑来判断是否允许数据包通过，然而包过滤防火墙允许内、外网的计算机直接建立连接，电路级网关防火墙则不允许 TCP 端到端的连接，而是要建立两个连接。其中一个连接是网关到内部主机，另一个是网关到外部主机。一旦两个连接被建立，网关只简单地进行数据中转，即它只在内部连接和外部连接之间来回复制字节，并将源 IP 地址转换为自己的地址，使得外界认为是网关和目的地址在进行连接。由于电路级网关在会话建立连接后不对所传输的内容作进一步的分析，因此安全性稍低。

电路级网关防火墙的工作原理如图 6-7 所示。

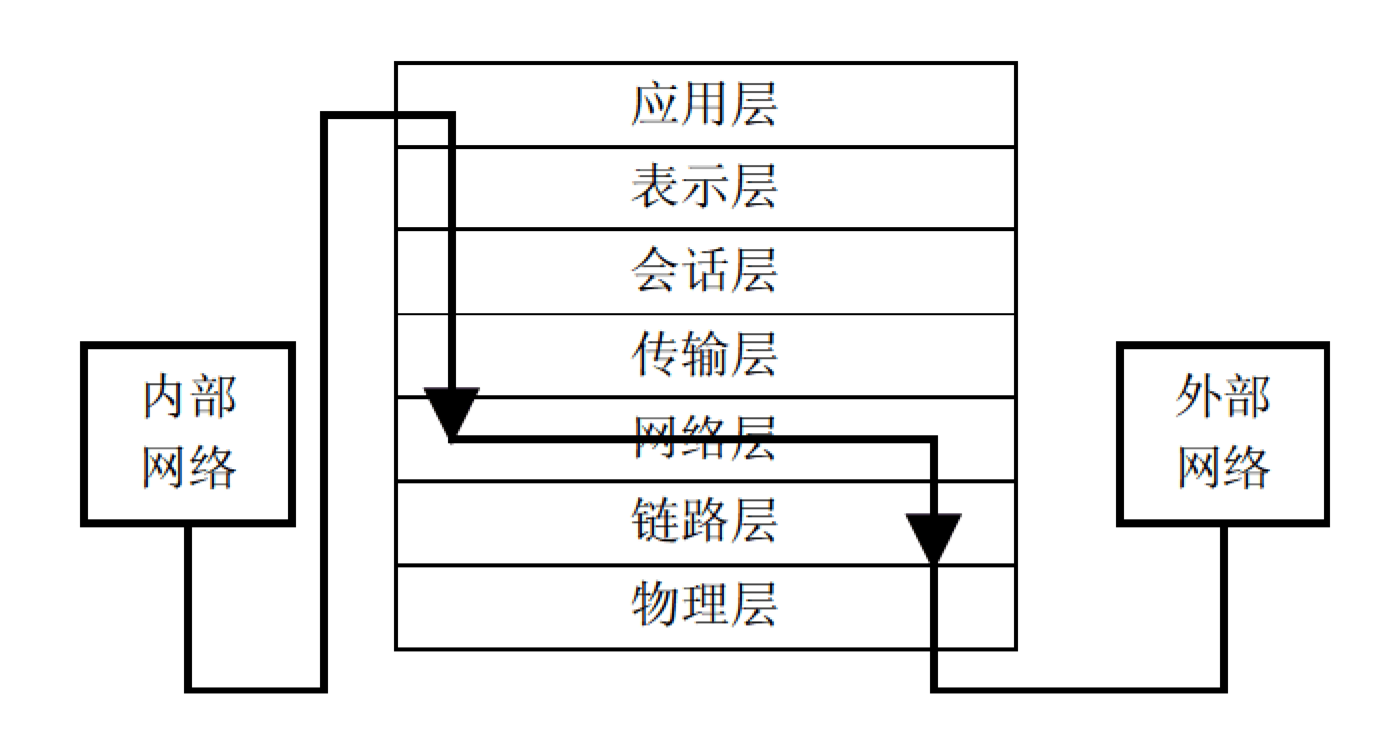


图 6-7　电路级网关防火墙工作原理

4. 代理服务技术的优点

（1）代理易于配置

代理因为是一个软件，所以它较过滤路由器更易配置，配置界面十分友好。如果代理实现得好，可以对配置协议要求较低，从而可以避免一些配置错误。

（2）代理能生成各项记录

因代理工作在应用层，并检查各项数据，因此可按一定准则让代理生成各项日志、记录。这些日志、记录对于流量分析、安全检查是十分重要的。当然，也可以用于记费等应用。

（3）代理能灵活、完全地控制进出流量、内容

通过采取一定的措施，按照一定的规则，用户可以借助代理实现一整套的安全策略。例如，可以控制“谁”和“什么”，还有“时间”和“地点”。

（4）代理能过滤数据内容

用户可以把一些过滤规则应用于代理，让它在高层实现过滤功能，例如文本过滤、图

像过滤（目前还未实现，但这是一个热点研究领域）、预防病毒或扫描病毒等。

（5）代理能为用户提供透明的加密机制

用户通过代理输入/输出数据，可以让代理完成加解密的功能，从而方便用户，确保数据的机密性。这一点在虚拟专用网中特别重要。代理可以广泛地用于企业外部网中，提供较高安全性的数据通信。

（6）代理可以方便地与其他安全手段集成

目前的安全问题解决方案很多，例如认证（Authentication）、授权（Authorization）、账号（Accounting）、数据加密、安全协议 SSL 等。如果把代理与这些手段联合使用，将大大增加网络安全性。这也是近期网络安全的发展方向。

5. 代理服务技术的缺点

（1）代理速度较路由器慢

路由器只是简单查看 TCP/IP 报头，检查特定的几个域，不作详细分析、记录；而代理工作于应用层，要检查数据包的内容，按特定的应用协议（例如 HTTP）进行审查、扫描数据包内容，并进行代理（转发请求或响应），故其速度较慢。

（2）代理对用户不透明

许多代理要求客户端作相应改动或安装定制客户端软件，这给用户增加了不透明度。由于硬件平台和操作系统都存在差异，要为庞大的异构网络的每一台内部主机安装和配置特定的应用程序既耗费时间，又容易出错。

（3）对于每项服务代理可能要求不同的服务器

可能需要为每项协议设置一个不同的代理服务器，因为代理服务器不得不理解协议以便判断什么是允许的和什么是不允许的，并且还要扮演一个对真实服务器来说是客户、对代理客户来说是服务器的角色。挑选、安装和配置所有这些不同的服务器，也可能是一项工作量较大的工作。

（4）代理服务不能保证免受所有协议弱点的限制

作为一种解决安全问题的方法，代理的成效取决于其对协议中哪些是安全操作的判断能力。每个应用层协议都或多或少存在着一些安全问题，对于一个代理服务器来说，要彻底避免这些安全隐患几乎是不可能的，除非关掉这些服务。

此外，代理的成效还取决于在客户端和真实服务器之间插入代理服务器的能力，这要求两者之间交流的相对直接性，而且有些服务的代理是相当复杂的。

（5）代理不能改进底层协议的安全性

因为代理工作于 TCP/IP 之上，属于应用层，也就无法改善底层通信协议的安全防范能力（例如 IP 欺骗、伪造 ICMP 消息和一些拒绝服务的攻击）。而这些方面，对于一个网络的健壮性来说是相当重要的。

6. 两种防火墙技术的对比

两种防火墙技术的对比，如表 6-1 所示。

表 6-1 两种防火墙技术的对比

	包过滤防火墙	代理防火墙
优点	价格较低	内置了专门为提高安全性而编制的代理应用程序，能够透彻地理解相关服务的命令，对来往的数据包进行安全化处理
	工作在网络和传输层，所以处理数据包的速度快、效率高	不允许数据包直接通过火墙，避免了数据驱动式攻击的发生，安全性好
	提供透明的服务，用户不用改变客户端程序	能生成各项记录；能灵活、完全地控制进出的流量和内容；能过滤数据内容
缺点	定义复杂，容易出现因配置不当带来的问题	对于每项服务，代理可能要求不同的服务器
	允许数据包直接通过，存在遭受数据驱动式攻击的潜在危险	速度较慢
	不能彻底防止地址欺骗	对用户不透明，用户需要改变客户端程序
	数据包中只有来自哪台机器的信息，不包含来自哪个用户的信息，不支持用户认证	不能保证免受所有协议弱点的限制
	不能理解特定服务的上下文环境，相应控制只能在高层由代理服务和应用层网关来完成	速度较慢，不太适用于高速网（ATM 或千兆位 Intranet 等）之间的应用
	不提供日志功能	不能改进底层协议的安全性

通过对代理服务器和包过滤器进行比较，了解它们提供的网络安全有什么不同也是非常必要的。

（1）代理服务器对整个 IP 数据包的数据进行扫描，因此能够比包过滤器提供更详细的日志文件。

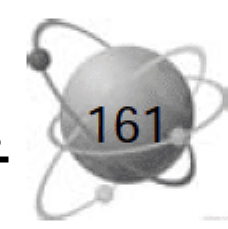
（2）如果数据包和包过滤规则匹配，就允许数据包通过防火墙；而代理服务器要用新的源 IP 地址重建数据包，这样对外隐藏了内部用户。

（3）使用代理服务器，意味着在 Internet 上必须有一个服务器，且内部主机不能直接与外部主机相连，因此带有恶意攻击的外部数据包也就不能到达内部主机。

（4）对网络通信而言，如果包过滤器由于某种原因不能工作，可能出现的结果是所有的数据包都能到达内部网；而如果代理服务器由于某种原因不能工作，整个网络通信将被终止。

6.2.4 状态检测技术

为了克服基本包过滤模式所带有的明显安全问题，一些包过滤防火墙厂商提出了所谓的状态包检测（Stateful Inspection）概念。上面提到的包过滤技术简单地查看每一个单一的输入包信息，而状态包检测模式则增加了更多的包和包之间的安全上下文检查，以达到与应用级代理防火墙相类似的安全性能。状态包检测防火墙在网络层拦截输入包，并利用足够的企图连接的状态信息作出决策（通过对高层的信息进行某种形式的逻辑或数学运算），如图 6-8 所示。



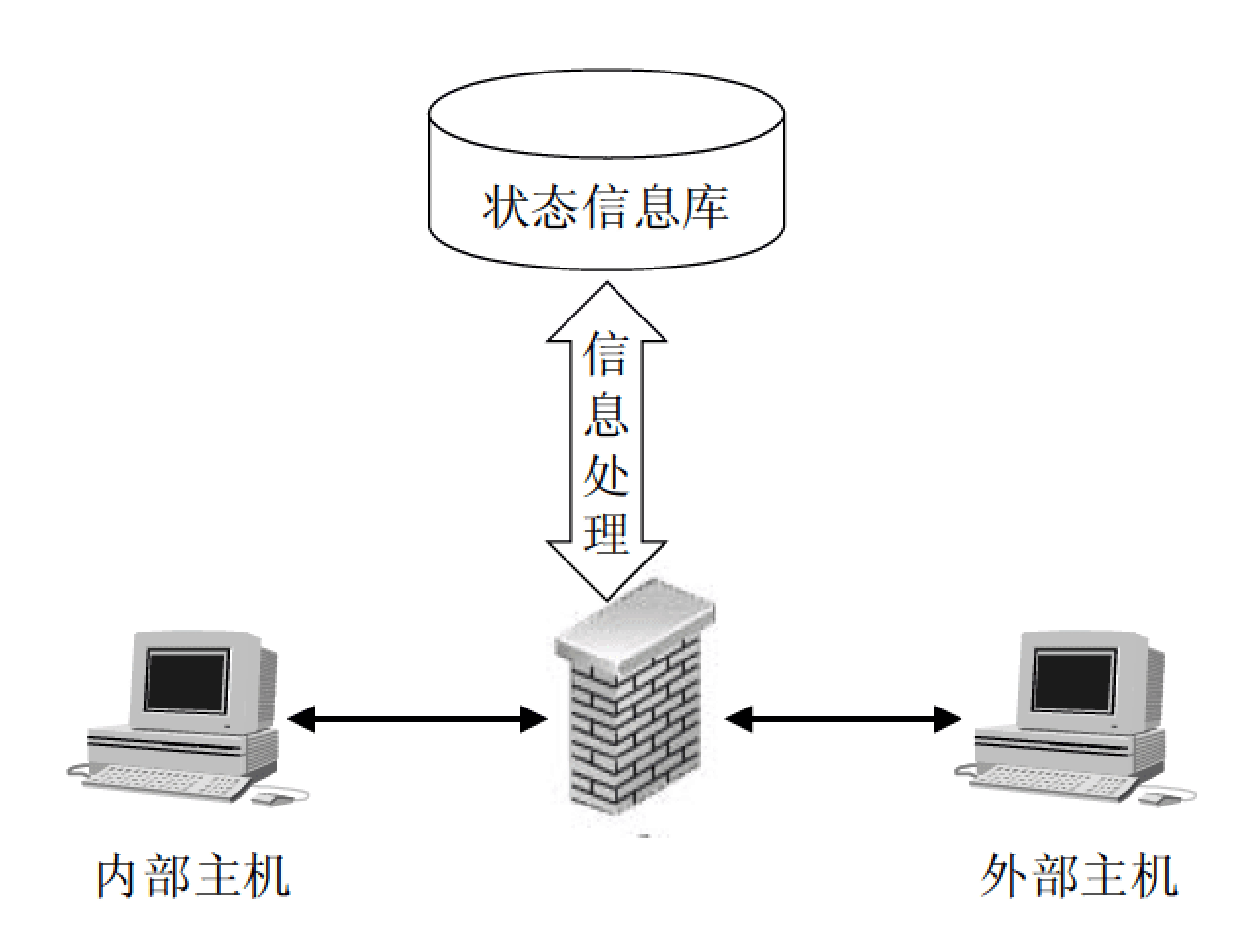


图 6-8　状态包检测防火墙

这些包在操作系统内核的私有检测模块中进行检测。安全决策所需的相关状态信息在检测模块中进行检测，然后保留在评价后续连接企图的动态状态表（库）中。被检查通过的包发往防火墙内部，允许直接连接内部、外部主机系统。

状态包检测防火墙工作在协议栈的较低层，通过防火墙的所有数据包都在低层进行处理，不需要协议栈的上层来处理任何数据包，因此减少了高层协议头的开销，执行效率也大大提高了。

另外，一旦一个连接在防火墙中建立起来，就不用再对该连接进行更多的处理。这样系统就可以去处理其他连接，执行效率可以得到进一步的提高。尽管状态包检测防火墙显著地增强了简单包过滤防火墙的安全性，但它仍然不能提供和前面提及的应用级检测相似的充足能见度。状态包检测防火墙不依靠与应用层有关的代理，而是依靠某种算法来识别进出的应用层数据，即根据已知合法数据包来比较进出防火墙的数据包，这样从理论上就能比应用级代理在过滤数据包上更加有效。但应用级代理防火墙对最高层的协议栈内容有足够的能见度，从而可以准确地知道它的意图，而状态包检测防火墙必须在没有这些信息的情况下作出安全决策。

例如，当应用级代理防火墙厂商声称支持微软 SQL Server 时，任何到内部 SQL Server 服务器的远程连接必须在应用层通过专门的微软 SQL 代理接受全面的检测；而对于状态包检测防火墙，允许远程用户访问防火墙后面的 SQL 数据库肯定要冒极大的安全风险。

带有状态检测的包过滤防火墙仍然允许外部用户直接访问内网系统和应用程序，而这些程序和系统可能配置在拥有众所周知的安全弱点的操作系统上。应用级代理通过一个自身具有有限、明确任务集的代理来限制访问应用程序或计算机系统，从而克服了这些同样的弱点。因此，应用级代理防火墙提供了比包过滤防火墙更多的安全性。

6.2.5　自适应代理技术

自适应代理（Adaptive Proxy）防火墙技术，从本质上来讲也属于代理服务技术，但它还结合了动态包过滤（状态包检测）技术。

自适应代理技术是较新的一种防火墙设计，它将前几代防火墙的优点合成到一个单一的完整系统中并使它们的弱点缩减到最小。对于自适应代理服务器来说，基本的安全检测仍在应用层进行，但一旦安全检测代理明确了会话的所有细节，那么其后的数据包就可以直接经过速度更快的网络层。因此，自适应代理防火墙基本上和标准代理服务防火墙一样安全，并且比状态包检测有更快的性能。

自适应代理防火墙也比标准的代理防火墙更灵活，为安全管理者提供了更明确的控制以满足他们的特殊需求，从而使“速度和安全”的折中处于最佳状态。

组成这种类型防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server，APS）与动态包过滤器。在自适应代理与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应代理的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求或是从网络层转发数据包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。所以，它结合了应用层网关防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高了 10 倍以上。

6.3 防火墙的体系结构

目前，防火墙的体系结构一般有屏蔽路由器体系结构、双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构 4 种。

6.3.1 屏蔽路由器体系结构

屏蔽路由器（Screening Router，SR）又称为包过滤路由器，是最简单也是最常见的防火墙。屏蔽路由器作为内外连接的唯一通道，要求所有的报文都必须在此通过检查；它除了具有路由功能外，还可安装包过滤软件，利用包过滤规则完成基本的防火墙功能，如图 6-9 所示。

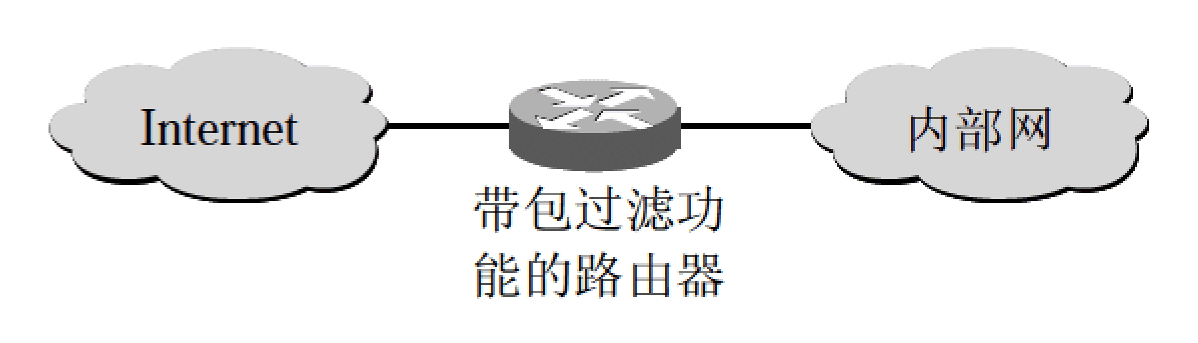


图 6-9 屏蔽路由器体系结构

屏蔽路由器可以由厂家专门生产的路由器实现，也可以用主机来实现。

这种配置的缺点在于：

（1）没有或有很少的日志记录能力，因此网络管理员很难确定系统是否正在被入侵或已经被入侵了。

（2）规则表随着应用的不断深化，将会很快变得很大而且复杂。

（3）这种防火墙的最大弱点是依靠一个单一的部件来保护系统，一旦部件出现问题，会使网络的大门敞开，而用户可能还不知道。

6.3.2　双重宿主主机体系结构

双重宿主主机（Dual Homed Host，DHH）体系结构是围绕具有双重宿主的堡垒主机构筑的，该堡垒主机至少有两块网卡。这样的堡垒主机可以充当与其所带网卡相连的网络之间的路由器，能够从一块网卡到另一块网卡转发 IP 数据包。但是，实现双重宿主主机的防火墙体系结构禁止这种转发功能，因此在拥有这种防火墙体系结构的网络中，IP 数据包并不是直接从一个网络（例如因特网）发送到其他网络（例如内部的、被保护的网络）的。

也就是说，防火墙内部的系统能与双重宿主主机通信，同时防火墙外部的系统（在因特网上）也能与双重宿主主机通信，但是这些系统之间不能直接互相通信，它们之间的 IP 通信被完全阻止。

双重宿主主机的防火墙体系结构是相当简单的：双重宿主主机位于两者之间，并且被分别连接到因特网和内部网络，如图 6-10 所示。

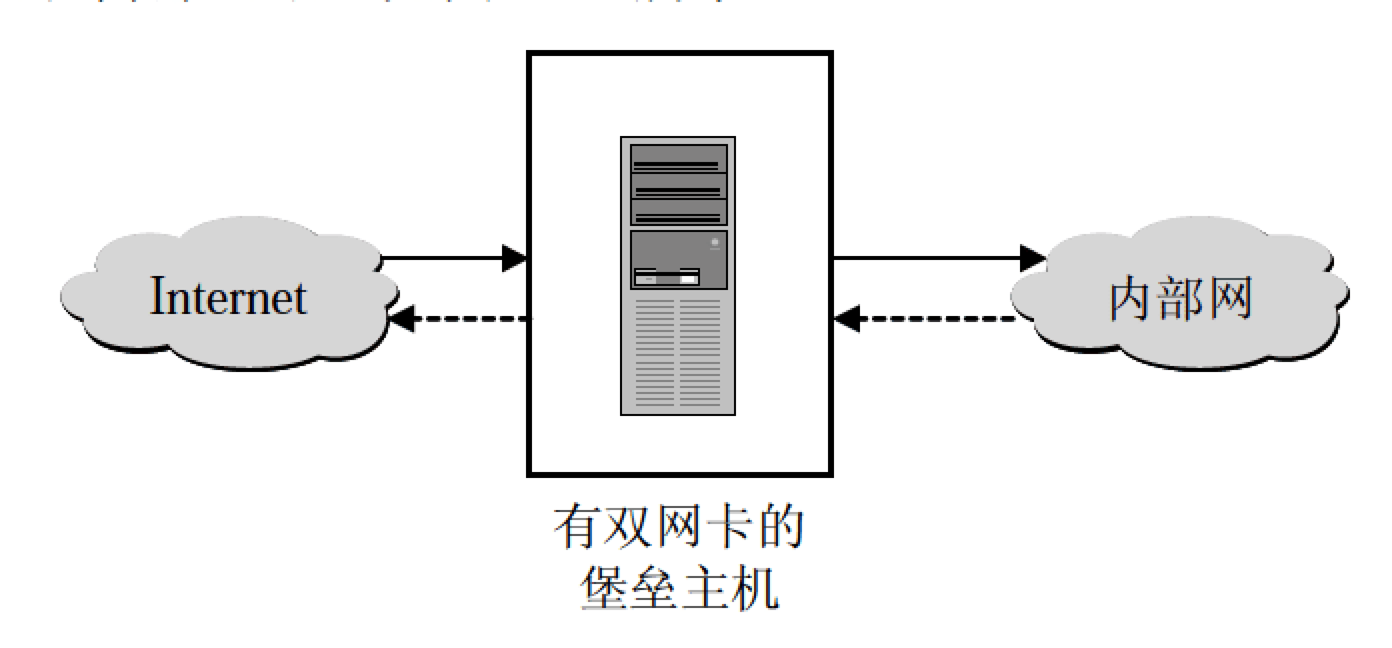


图 6-10　双重宿主主机体系结构

双重宿主主机网关优于屏蔽路由器的地方是：堡垒主机的系统软件可用于维护系统日志、硬件复制日志或远程日志。这对于日后的检查很有用，但尚不足以帮助网络管理者确认内部网中哪些主机可能已被黑客入侵。

双重宿主主机网关的一个致命弱点是：一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网上用户均可以随意访问内部网。

6.3.3　屏蔽主机体系结构

屏蔽主机网关（Screened Gateway，SG）由屏蔽路由器和应用网关组成，屏蔽路由器的作用是包过滤，应用网关的作用是代理服务，即在内部网络和外部网络之间建立了两道安全屏障，既实现了网络层安全（包过滤），又实现了应用层安全（代理服务）。

屏蔽主机网关很容易实现：在内部网络与因特网的交汇点安装一台屏蔽路由器，同时在内部网络上安装一台堡垒主机（应用层网关）即可，如图 6-11 所示。

值得注意的是，应用网关只有一块网卡，因此它不是双重宿主主机网关。

屏蔽主机网关防火墙具有双重保护，比双重宿主主机网关防火墙更灵活，安全性更高；但由于要求对两个部件进行配置以便能协同工作，所以防火墙的配置工作很复杂。

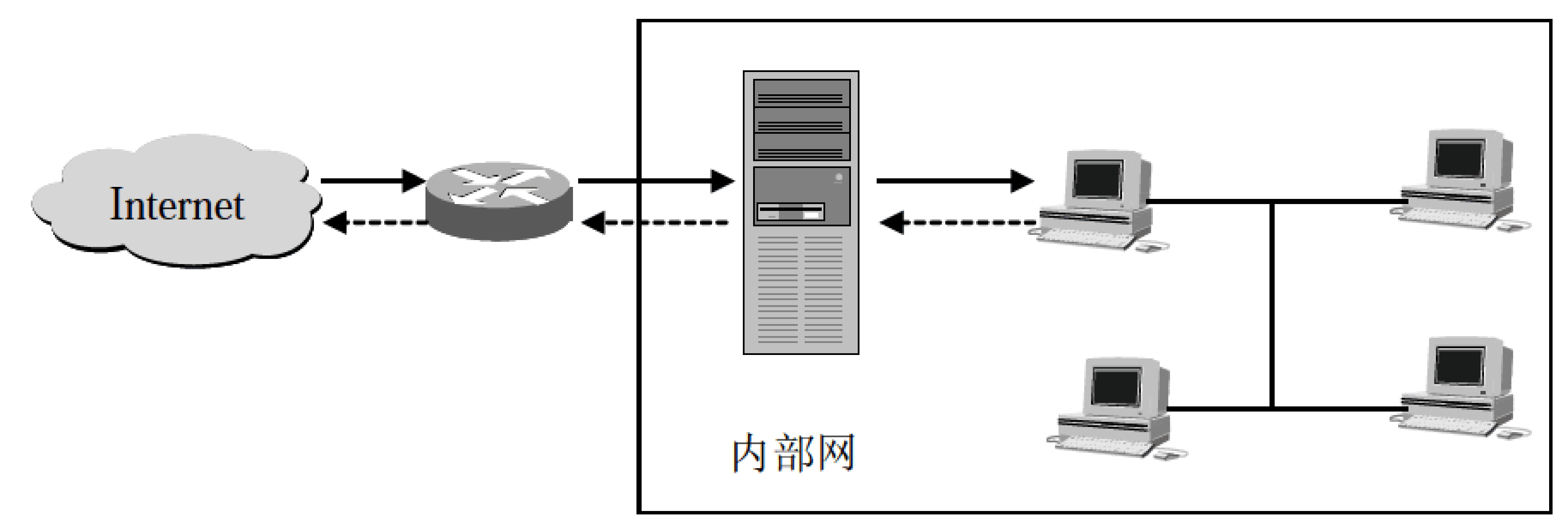


图 6-11 屏蔽主机体系结构

6.3.4 屏蔽子网体系结构

屏蔽子网（Screened Subnet，SS）防火墙是在屏蔽主机网关防火墙的基础上再加一个路由器，两个屏蔽路由器分别放在子网的两端，形成一个被称为隔离区或非军事区（Demilitarized Zone，DMZ）的子网，即在内部网络和外部网络之间建立一个被隔离的子网，如图 6-12 所示。

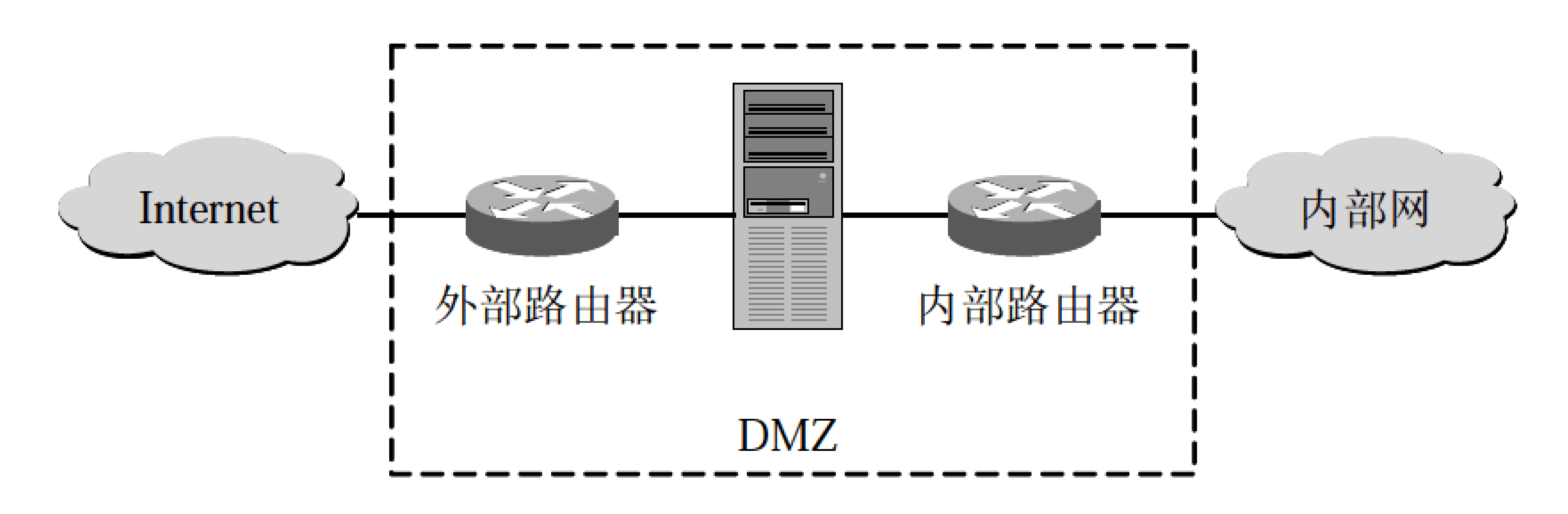


图 6-12 最简单的屏蔽子网体系结构

内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网进行通信，像 WWW 和 FTP 服务器等对外提供服务的服务器可放在 DMZ 中。有的屏蔽子网中还设有一台堡垒主机作为唯一可访问点，支持终端交互或作为应用网关代理。

这种配置的危险带仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。外部屏蔽路由器和应用网关与在屏蔽主机网关防火墙中的功能相同；内部屏蔽路由器在应用网关与受保护网络之间提供附加保护，从而形成 3 道防线。因此，一个入侵者要进入受保护的网络比主机过滤防火墙更加困难。

但是，它要求的设备和软件模块最多，其配置最贵且相当复杂。

6.3.5 组合体系结构

搭建防火墙时，一般很少采用单一的技术，通常采用解决不同问题的多种技术的组合。这种组合主要取决于网管中心想向用户提供什么样的服务、网管中心对网络安全等级的要求以及能够接受的风险；也取决于经费、投资的大小或技术人员的技术水平等因素。

1. 多堡垒主机

理想情况下，堡垒主机应该只提供一种服务，因为提供的服务越多，在系统上安装服务而导致安全隐患的可能性也就越大。这就意味着，如果在网络边界上拥有一个防火墙程序、一台 Web 服务器、一台 DNS 服务器和一台 FTP 服务器，那么就需要配置 4 台独立的堡垒主机。

使用如图 6-13 所示的多堡垒主机，可以改善网络安全性能、引入冗余度以及隔离数据和服务器。

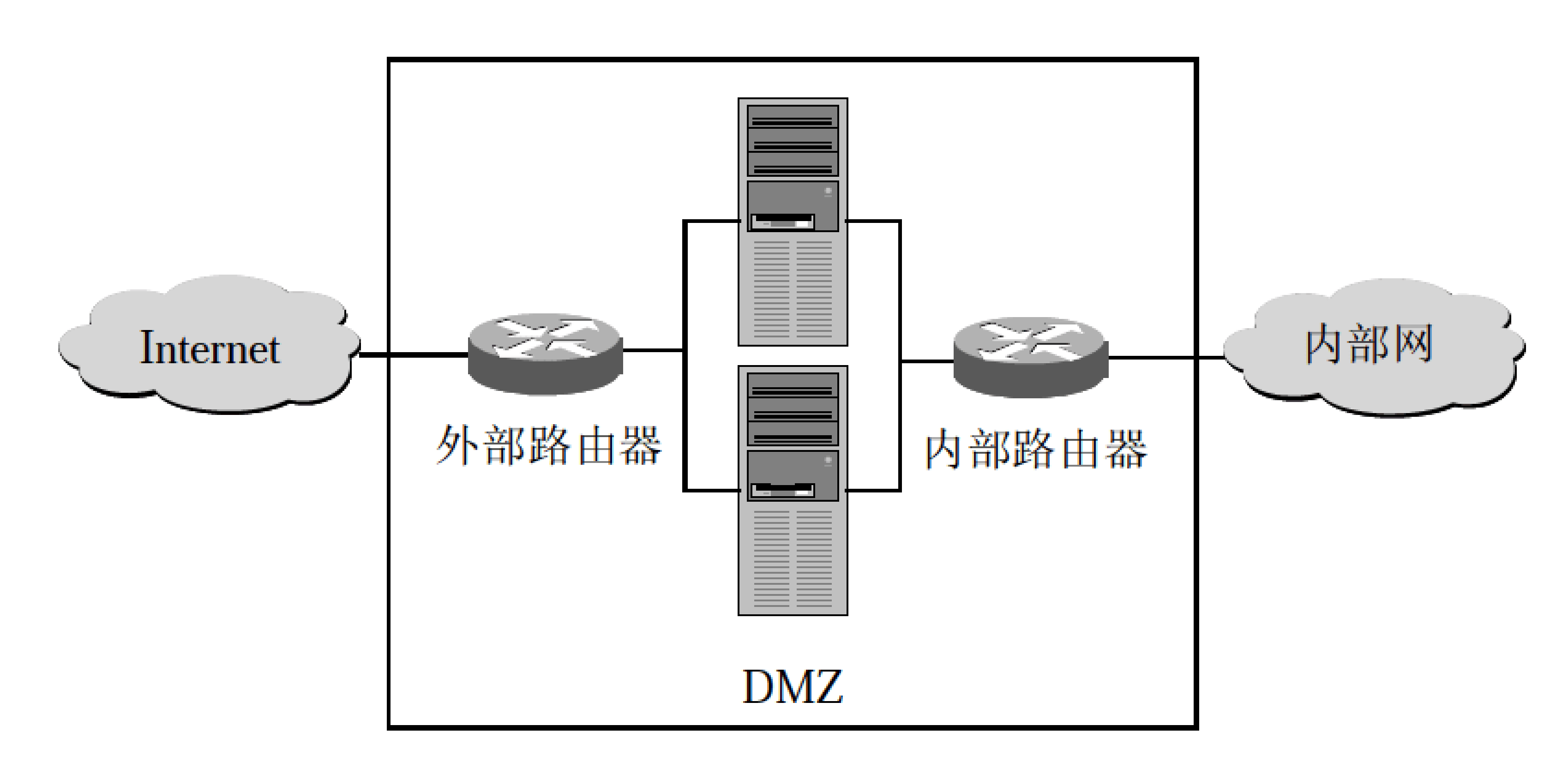


图 6-13　双垒主机的屏蔽子网体系结构

2. 合并内部路由器和外部路由器

通常屏蔽子网体系结构要求在子网两侧各使用一个路由器分别充当内部和外部路由器，在每个接口上设置入站和出站的过滤规则；而将两者合并后，就变成了如图 6-14 所示的体系结构。其优点是节约了路由器的开支，最主要的缺点是黑客只要攻破该路由器就可以进入内部网络。

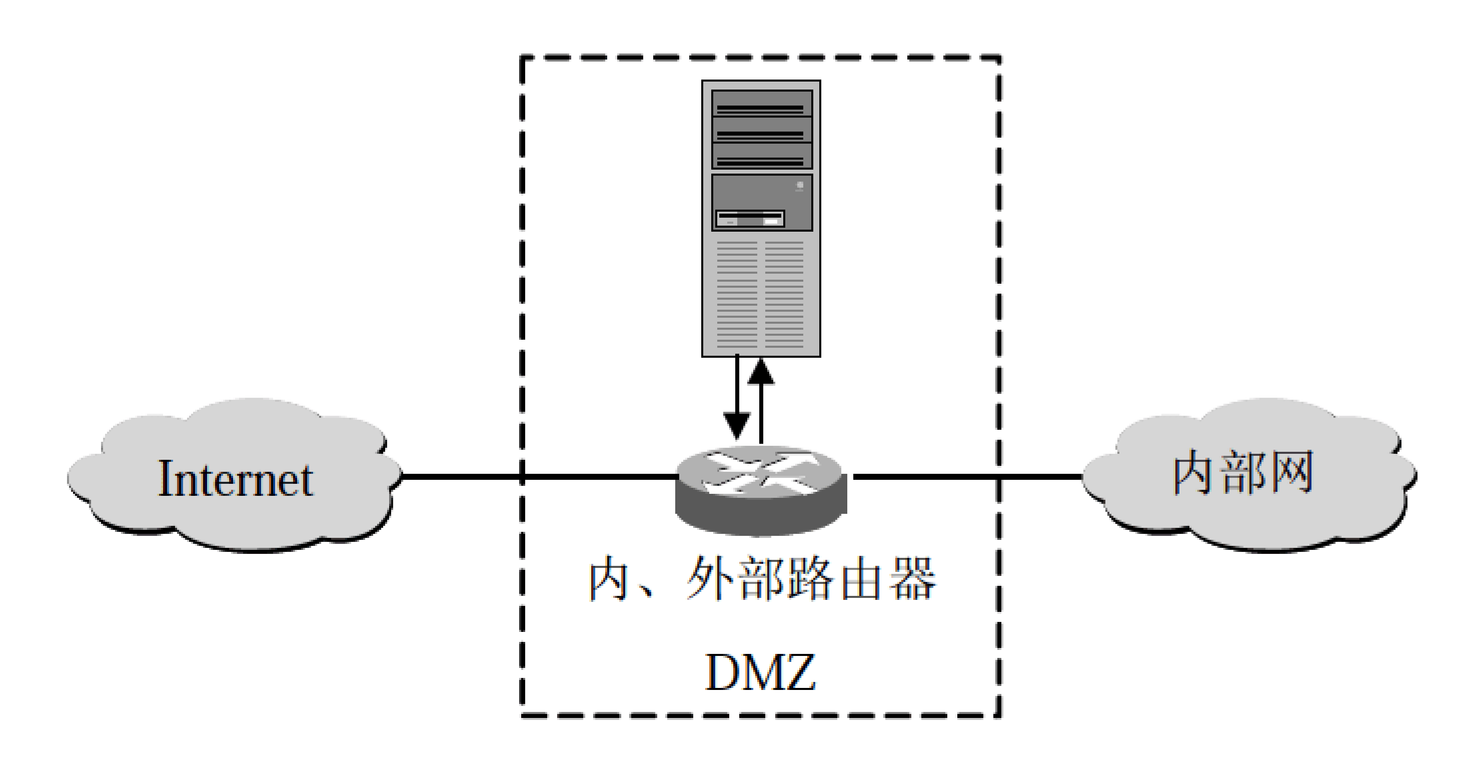


图 6-14　单个路由器的屏蔽子网体系结构

3. 合并堡垒主机和外部路由器

使用一个配有双网卡的主机，既做堡垒主机又充当外部路由器。在这种体系结构中，堡垒主机没有外部路由器的保护，直接暴露给了 Internet，安全性不好。

这种方案的唯一保护是堡垒主机自己提供的包过滤功能。当网络只有一个到 Internet

的拨号 PPP 连接，并且堡垒主机上运行了 PPP 数据包时，也可以选择这种设置方法。

堡垒主机充当外部路由器如图 6-15 所示。

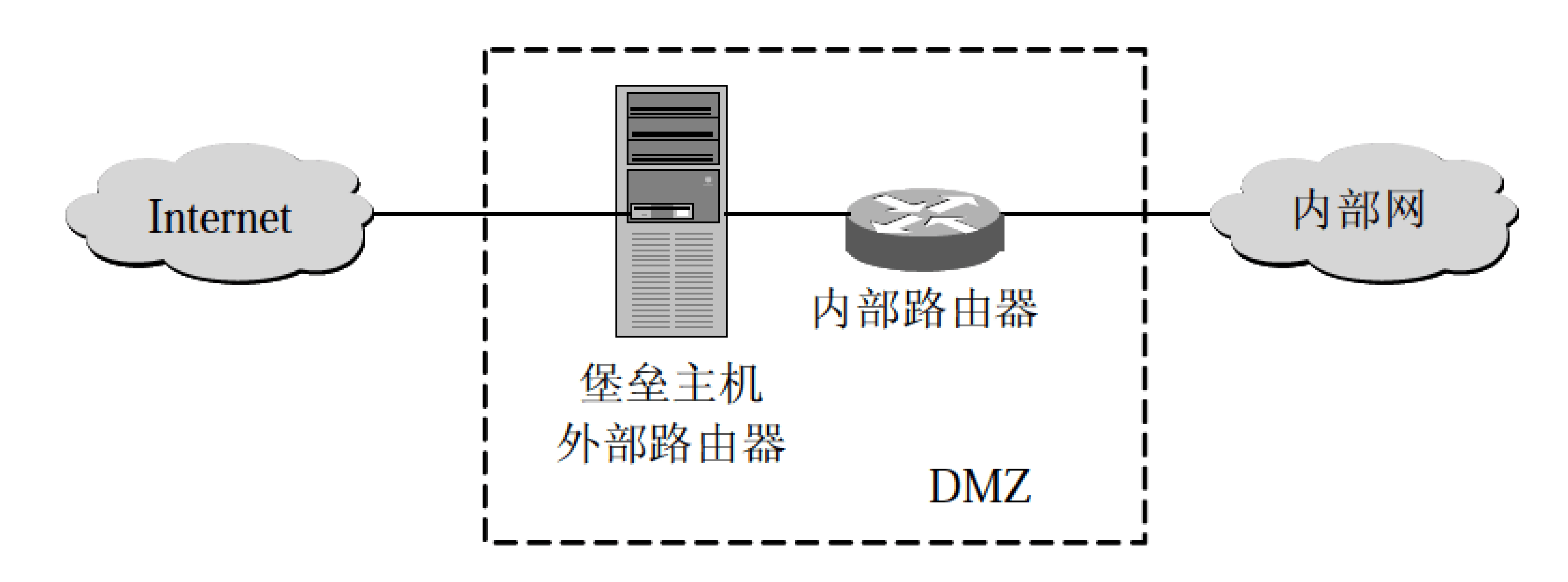


图 6-15 堡垒主机充当外部路由器

4. 合并堡垒主机和内部路由器

使用一个配有双网卡的主机，既做堡垒主机又充当内部路由器。此时，堡垒主机与内部网通信，以便转发从外部网获得的信息。

堡垒主机充当内部路由器如图 6-16 所示。

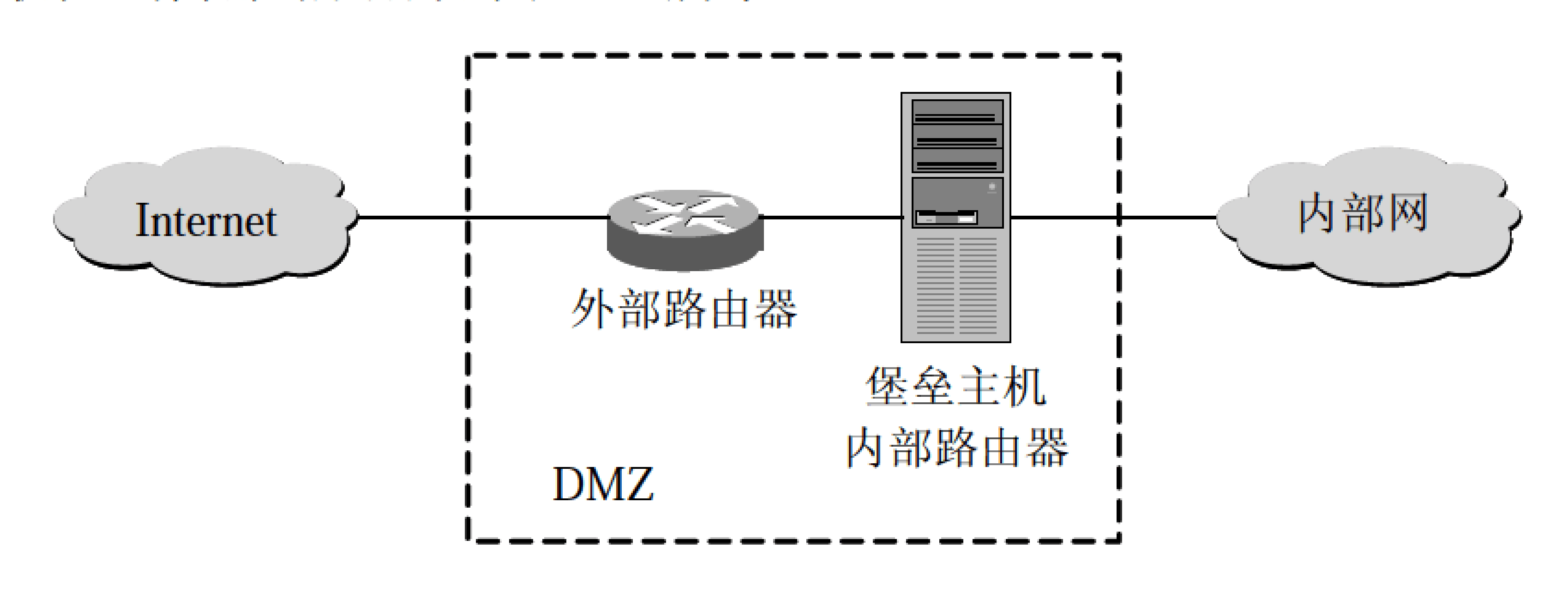


图 6-16 堡垒主机充当内部路由器

5. 使用多台外部路由器

如果内部网络既要连接到 Internet，同时还要并行地连接到分支机构或者合作伙伴的网络，就可以放置多台外部路由器，它们的工作方式与单台路由器相同。

当有两台外部路由器时，黑客攻入任一个路由器的机会就增加了一倍，多台亦然。

多台外部路由器的子网过滤体系结构如图 6-17 所示。

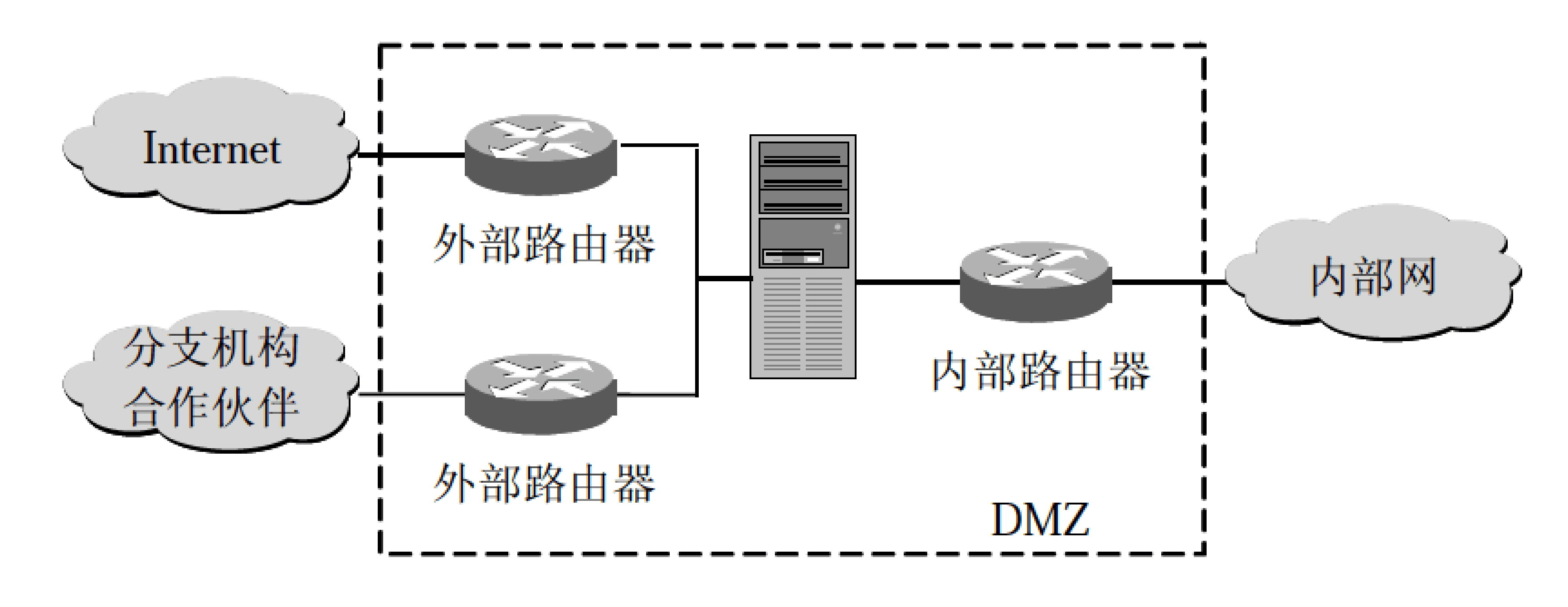


图 6-17 多台外部路由器的屏蔽子网过滤体系结构

6．使用多个周边网络

如果内部网络与分支机构及合作伙伴之间的网络有任务紧急的应用连接，需要并发处理，就可以使用多个 DMZ，以确保高可靠性和高安全性。

这种结构的优点是，提高了网络的冗余度，在数据传输中将不同的网络隔离开，增加了数据的保密性。

其缺点是，存在多个路由器，它们都是进入内部网的通道。如果不能严格地监控和管理这些路由器，就会给入侵者提供更多的机会。

有两个 DMZ 的屏蔽子网体系结构如图 6-18 所示。

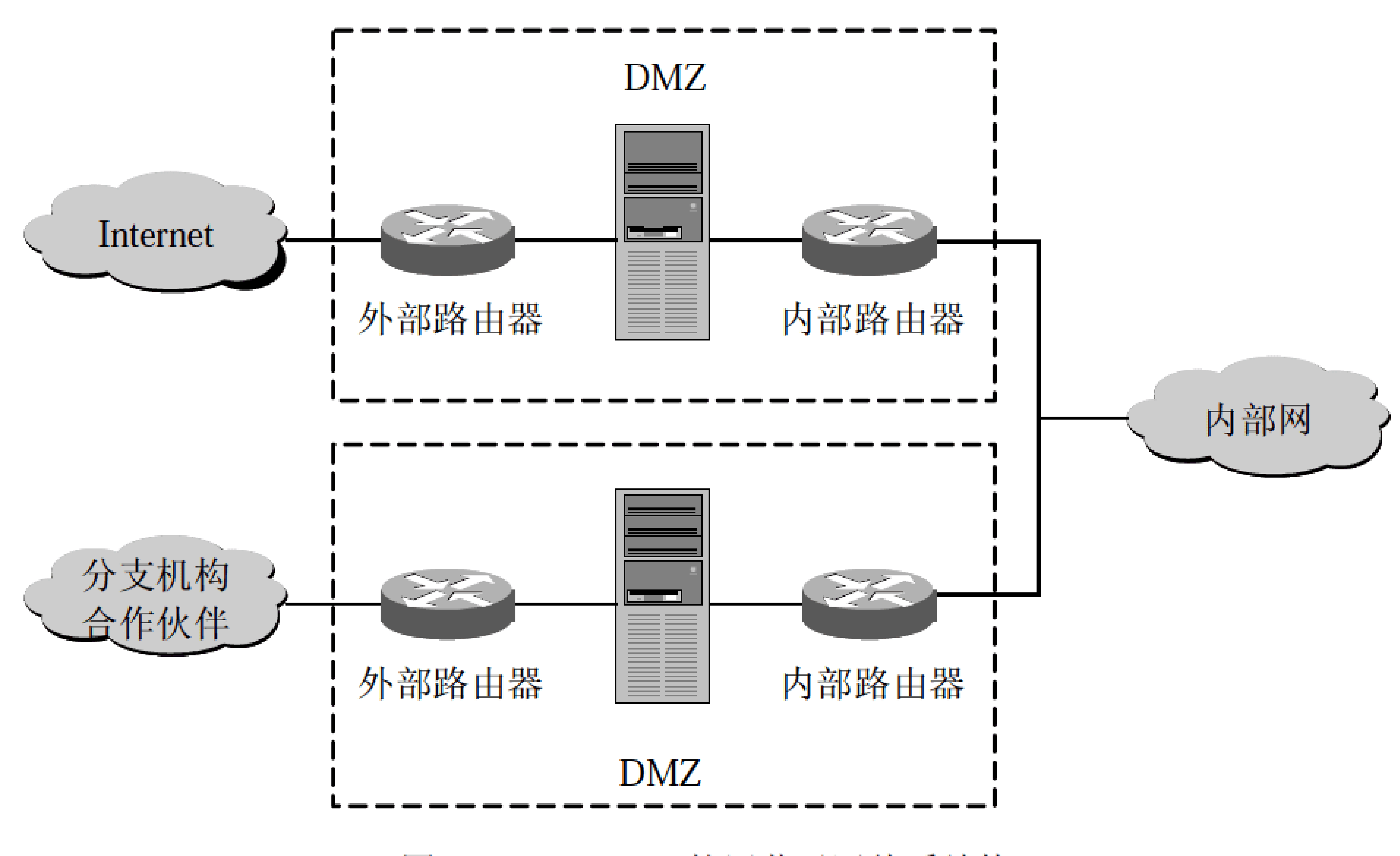


图 6-18　双 DMZ 的屏蔽子网体系结构

6.4　防火墙选型与产品简介

6.4.1　防火墙产品选购策略

防火墙系统可以说是网络的第一道防线，因此用户在决定使用防火墙保护内部网络的安全时，第一步要做的事情就是选购一个安全、实惠、合适的防火墙。而在市场上，防火墙的售价相差悬殊，从几万元到数十万元，甚至上百万元不等。因为各用户要求的安全程度不尽相同，因此厂商所推出的产品也就有所区分，甚至有些公司还推出类似模块化的功能产品，以满足各种不同用户的安全要求。面对种类如此繁多的防火墙产品，用户应该如何进行取舍呢？

首先，用户需要了解一个防火墙系统应具备的基本功能，这是用户选择防火墙产品的依据和前提；其次，选购防火墙时主要应该考虑安全性、高效性、适用性、可管理性和售后服务体系等因素。

1．防火墙的安全性

安全性是评价防火墙好坏最重要的因素，因为购买防火墙的主要目的就是为了保护网络免受攻击。但是安全性不像速度、配置界面那样直观、便于估计，往往被用户忽视。对于安全性的评估，需要配合使用一些攻击手段进行。

防火墙自身的安全性也很重要，大多数人在选择防火墙时都将注意力放在防火墙如何控制连接以及防火墙支持多少种服务上，而往往忽略了一点——防火墙也是网络上的主机之一，也可能存在安全问题，当防火墙主机上所运行的软件出现安全漏洞时，防火墙本身也将受到威胁，此时任何的防火墙控制机制都可能失效。因此，如果防火墙不能确保自身安全，则防火墙的控制功能再强，也不能完全保护内部网络。

2．防火墙的高效性

用户的需求是选购何种性能防火墙的决定因素。

用户安全策略中往往还可能会考虑一些特殊功能要求，但并不是每一个防火墙都会提供这些特殊功能的。用户常见的需求可能包括：

（1）网络地址转换功能 NAT

进行地址转换有两个优点：其一是可以隐藏内部网络真正的 IP 地址，使黑客无法直接攻击内部网络，这也是要强调防火墙自身安全性问题的主要原因；其二是可以使内部使用保留的 IP 地址，这对许多 IP 地址不足的企业是有益的。

（2）双重域名服务 DNS

当内部网络使用没有注册的 IP 地址或是防火墙进行 IP 地址转换时，DNS 也必须经过转换，因为同样的一台主机在内部的 IP 地址与给予外界的 IP 地址是不同的，有的防火墙会提供双重 DNS，有的则必须在不同主机上各安装一个 DNS。

（3）虚拟专用网络 VPN

VPN 可以在防火墙与防火墙或移动的客户端之间对所有网络传输的内容进行加密，建立一个虚拟通道，让两者感觉是在同一个网络上，可以安全且不受拘束地互相存取。

（4）杀毒功能

大部分防火墙都可以与防病毒软件搭配实现杀毒功能，有的防火墙甚至直接集成了杀毒功能。两者的主要差别只是后者的杀毒工作由防火墙完成，或由另一台专用的计算机完成。

（5）特殊控制需求

有时企业会有一些特别的控制需求，例如限制特定使用者才能发送 E-mail；FTP 服务只能下载文件，不能上传文件；限制同时上网的人数；限制使用时间或阻塞 Java、ActiveX 控件等，依需求不同而异。

防火墙的性能主要包括两个方面：最大并发连接数和数据包转发率。最大并发连接数是衡量防火墙可扩展性的一个重要指标。数据包转发率是指在所有安全规则配置正确的情况下，防火墙对数据流量的处理速度。购买防火墙的需求不同，对这两个参数的要求也不同。例如，一台用于保护电子商务 Web 站点的防火墙，支持越多的连接意味着能够接受越

多的客户和交易，所以防火墙能够同时处理多个用户的请求是最重要的，哪怕每个连接的流量很小；但是对于那些经常需要传输大的文件且对实时性要求比较高的用户，高的包转发率则是关注的重点。

3．防火墙的适用性

适用性是指量力而行。防火墙也有高低端之分，配置不同，价格不同，性能也不同。同时，防火墙有许多种形式，有的以软件形式运行在普通计算机之上，有的以硬件形式单独实现，也有的以固件形式设计在路由器之中。所以，在购买防火墙之前，用户必须了解各种形式防火墙的原理、工作方式和不同的特点，才能评估它是否能够真正满足自己的需要。

另外，用户挑选防火墙时，还应该考虑自身的因素。例如：

（1）用户网络受威胁的程度。

（2）若入侵者闯入网络，或由于硬件、软件失效，将要受到的潜在损失。

（3）其他已经用来保护网络及其资源的安全措施。

（4）希望能从 Internet 得到的服务以及可以同时通过防火墙的用户数目。

（5）站点是否有经验丰富的管理员。

（6）今后可能的要求，例如要求增加通过防火墙的网络活动或要求新的 Internet 服务等。

4．防火墙的可管理性

防火墙的管理是对安全性的一个补充。目前有些防火墙的管理配置需要有很深的网络和安全方面的专业知识，很多防火墙被攻破不是因为程序编码的问题，而是管理和配置错误导致的。

对管理的评估，可以从以下 3 个方面进行。

（1）远程管理

允许网络管理员对防火墙进行远程干预，并且所有远程通信需要经过严格的认证和加密。例如，管理员下班后出现入侵迹象，防火墙可以通过发送电子邮件的方式通知该管理员，管理员可以以远程方式封锁防火墙的对外网卡接口或修改防火墙的配置。

（2）访问控制规则的配置界面应该直观、使用简单

大多数防火墙产品都提供了基于 Web 方式或图形用户界面 GUI 的配置界面。

（3）日志文件不仅能够帮助用户追查攻击者的踪迹，还可以记录流量

防火墙的一些功能可以在日志文件中得到体现。防火墙提供灵活、可读性强的审计界面是很重要的。例如，用户可以查询从某一固定 IP 地址发出的流量、访问的服务器列表等，因为攻击者可以采用不停地填写日志以覆盖原有日志的方法使追踪无法进行，所以防火墙应该提供设定日志大小的功能，同时在日志已满时给予提示。

因此，最好选择拥有界面友好、易于编程的 IP 过滤语言及便于维护管理的防火墙。

5．完善、及时的售后服务体系

只要有新的产品出现，就会有人研究新的破解方法，所以好的防火墙产品应拥有完善、

及时的售后服务体系。防火墙和相应的操作系统应该用补丁程序进行升级，而且升级必须定期进行。

总之，目前没有任何一个防火墙的设计能够适用于所有的环境，所以用户在选购防火墙时不要把防火墙的等级看得过重，而应根据网络站点的特点来选择合适的防火墙，能够满足安全要求即可，不要盲目追求高性能。

最后需要强调的是，虽然防火墙在当今 Internet 上的存在是有生命力的，但并不意味着能够替代其他安全措施。也就是说，它不是解决所有网络安全问题的万能药方，而只是网络安全策略中的一个组成部分，这是用户在决定购买防火墙产品之前就应该明确的问题。

6.4.2 典型防火墙产品介绍

目前国外比较知名的防火墙产品有 Check Point 公司的 FireWall-1，它所采用的访问控制规则集非常完善，同时提供良好的用户界面；Cisco 公司的 PIX 防火墙采用自适应性安全算法（Adaptive Security Algorithm），性能优良；NAI 公司的 Gaunlet 防火墙性能良好，NAI 公司还提出了一种自适应防火墙，将状态包过滤和应用代理技术互补使用；其他还包括 Cyberguard 公司的 Cyberguard Firewall 和 Netscreen 的 Netscreen-100 等。国内比较知名的防火墙产品包括北大青鸟公司的网关防火墙，特点是技术新、配置简单、安全性好；还有天融信公司的网络卫士防火墙和东大阿尔派公司的网眼防火墙等。

一个成功的防火墙产品应该具有以下基本功能。

（1）防火墙的设计策略应遵循安全防范的基本原则——“除非明确允许，否则就应该禁止”。

（2）防火墙本身支持安全策略，而不是添加上去的。

（3）如果组织机构的安全策略发生改变，可以加入新的服务。

（4）有先进的认证手段或有挂钩程序，可以安装先进的认证方法。

（5）如果需要，可运用过滤技术允许和禁止服务。

（6）可以使用 FTP 和 Telnet 等服务代理，以便先进的认证手段可以被安装和运行在防火墙上。

（7）拥有界面友好、易于编程的 IP 过滤语言，并可以根据数据包的性质进行包过滤。数据包的性质有源和目的 IP 地址、协议类型、源和目的 TCP/UDP 端口、TCP 包的 ACK 位、出站和入站网络接口等。

下面简单介绍一下 3Com、Cisco 和 Check Point 等公司的一些典型防火墙产品。

1. 3Com Office Connect Firewall

3Com Office Connect 系列 Internet 防火墙产品为小企业提供确保网络安全的廉价和高效的方法。经过 ISCA 认证的这种防火墙能拒黑客于门外，还可以用来控制局域网对 Internet 的使用（如禁止用户访问不恰当的资料，记录哪些站点最常被访问，以及 Internet 连接使用了多大的带宽）。其产品特性如下。

（1）新增的网络管理模块使技术经验有限的用户也能保障其商业信息的安全。

（2）Office Connect Internet Firewall 使用全静态数据包检验技术来防止非法的网络接入和防止来自 Internet 的“拒绝服务”攻击，它还可以限制局域网用户对 Internet 的不恰当使用。

（3）Office Connect Internet Firewall DMZ 可支持多达 100 个局域网用户，整个办公室可以共享 ISP 提供的一个 IP 地址，从而节省开支；局域网上的公共服务器既可以被 Internet 访问，又不会使局域网遭受攻击。

（4）3Com 公司所有的防火墙产品很容易通过 Getting Started Wizard 进行安装，使用方便。

2．Cisco PIX 防火墙

Cisco 防火墙与众不同的特点是基于硬件，而硬件产品的最大好处就是速度快。众所周知，防火墙的安全性和速度是一对矛盾，而采用大型专用集成芯片便可化解这对矛盾，从而解决防火墙的速度瓶颈问题，这对于网络中心和银行用户而言极为重要。Cisco PIX Firewall 便是这类产品，其包转换速度高达 170Mbps，同时可处理 6 万多个连接。

将防火墙技术集成到路由器中是 Cisco 网络安全产品的另一大特色。Cisco 在路由器市场的占有率达到 80%，在路由器的 IOS 中集成防火墙技术是其他厂家无可比拟的。这样做的好处是用户无须另外购置防火墙，可降低网络建设的总成本；而且它还可以通过网络远程下载，提供一种动态的网络安全保护。其产品特性如下：

（1）实时嵌入式操作系统。

（2）保护方案基于自适应安全算法 ASA，可以确保最高的安全性。

（3）用于验证和授权的“直通代理”技术。

（4）最多支持 250000 个同时连接。

（5）URL 过滤。

（6）HP Open View 集成。

（7）通过电子邮件和寻呼机提供报警。

（8）通过专用链路加密卡提供 VPN 支持。

（9）符合委托技术评估计划 TTAP，经过了美国安全事务处 NSA 的认证，同时通过了中国公安部安全检测中心的认证（PIX520 除外）。

其中，PIX Firewall 520 的处理性能是最好的，其吞吐量可达 150Mbps，而且使用 NAT 时不影响性能。它可以防止有害的 SMTP 命令，但对 FTP，它不能对 get 和 put 进行限制。PIX 的管理通过 Web 来进行，但使用 Web 界面管理 PIX 只能进行简单的配置。其日志和监控能力较弱，所有日志必须送到另一台运行 syslog 的机器上。

3．Check Point FireWall-1

Check Point 软件技术有限公司成立于 1993 年，国际总部在以色列的莱莫干市，美国总部位于加利福尼亚州红木城。该公司是 Internet 安全领域的全球领先企业，Check Point 已经成为防火墙软件的代名词，其推出并持有专利的状态监测技术是网络安全技术的事实标准。状态监测可提供准确而高效的业务量监测，并可对应用层的信息进行检查，从而提

供最高水平的安全性。由于状态监测无须单独的代理来保证每一项服务的提供，所以客户能够获得更高的性能、可伸缩性和业务能力。

Check Point 成名的部分原因归功于其安全性开放式平台（Open Platform for Security，OPSEC）。OPSEC 联盟成立于 1997 年，Check Point 当时的想法是向用户提供完整的、能够在多厂商之间进行紧密集成的网络安全解决方案。目前世界上许多著名的大公司，例如 IBM、HP、Cisco、3Com、BAY Networks 等，都已经成为 OPSEC 的成员，而其合作伙伴超过了 300 个。OPSEC 联盟分为两大部分：一部分 IT 厂商提供集成的应用程序，即被 Check Point OPSEC 认可的并且与 OPSEC 构架兼容的产品；另一部分提供基于 Check Point 平台的安全服务，这部分厂商向用户提供基于 Check Point 解决方案的硬盒子产品以及互联网设备和服务器。

FireWall-1 是 Check Point 众多网络安全产品中最重要的之一，也是业界领先的企业级安全性套件。它集成了访问控制、用户认证、NAT、VPN、内容安全性、审计和报告等特性。OPSEC 框架为 FireWall-1 和许多第三方安全应用提供了集成能力和企业级管理能力。

FireWall-1 的基本模块有：

（1）状态检测模块（Inspection Module）：提供访问控制、客户机认证、会话认证、NAT 和审计功能。

（2）防火墙模块（Firewall Module）：包含一个状态检测模块，另外提供用户认证、内容安全和多防火墙同步功能。

（3）管理模块（Management Module）：对一个或多个安全策略执行点（安装了 FireWall-1 的某个模块，例如状态检测模块、防火墙模块或路由器安全管理模块等的系统）提供集中的、图形化的安全管理功能，一个管理模块可以控制多达 50 个单独的 FireWall-1。

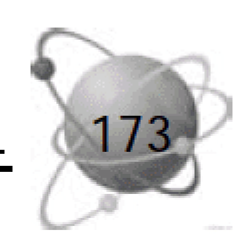
FireWall-1 支持两个平台：UNIX、Windows。FireWall-1 具有一种很特别的结构，称为多层次状态监视结构。这种结构使 FireWall-1 可以对复杂的网络应用软件进行快速支持。也因为这个功能，使得 Check Point 在防火墙产品市场中位居领导地位，有很多第三方厂商对它进行支持。而 Check Point 也提供了一套 API 供开发者使用，以便开发更多的辅助工具。

4. AXENT Raptor

Raptor 是最优秀的代理型防火墙之一。其界面易读、易操作，在实时日志方面，仅次于 FireWall-1。Raptor 的优势在于其代理的深度和广度。它提供对多种操作系统服务器的保护，还具有 SQL*NET 代理功能，可控制对 Oracle 数据库的访问。Raptor 在 SMTP 方面做得很好，而且它是唯一可防止缓存溢出的防火墙。另外，它还可以代理网络新闻传输协议 NNTP 和网络时间协议 NTP。

5. CyberGuard Firewall

CyberGuard Firewall 是由 CyberGuard 公司开发的，其主要结构是基于 CX/SX 多层式安全操作系统的，操作简单，很容易上手。CyberGuard Firewall 与其他防火墙产品不同的地方在于，它提供一种可以安装在防火墙上的加密卡。通过加密卡，可以进行硬件加密，这对于整体性能有显著的提高。另外，它还支持网络地址转换、Sock、分布式 DNS 等。



6．东软 NetEye

于 1991 年在东北大学创立的东软集团是中国领先的软件与解决方案提供商。东软 NetEye 防火墙基于专门的硬件平台，使用专有的 ASIC 芯片和专有的操作系统，基于状态包过滤的“流过滤”体系结构。围绕流过滤平台，东软构建了网络安全响应小组、应用升级包开发小组、网络安全实验室，不仅带给用户高性能的应用层保护，还包括新应用的及时支持、特殊应用的定制开发、安全攻击事件的及时响应等。

6.4.3　防火墙选型举例

由于用户数量、安全要求、功能要求不尽相同，市场上防火墙的售价相差悬殊，从数万元到数十万元，甚至到数百万元不等。网络吞吐量、丢包率、延迟、连接数等都是重要的技术指标。质量好的防火墙能够有效地控制通信，能够为不同级别、不同需求的用户提供不同的控制策略。控制策略的有效性、多样性、级别目标清晰性以及制定难易程度都直接反映出防火墙控制策略的质量。

1．小型办公和家用网络

小型、家庭办公和家用网络（Small Office Home Office，SOHO）要管理的用户和机器比较少，而且只需要访问极少量的 Internet 服务，例如电子邮件、Web 以及有时需要的流媒体。在这种情形下，简单的数据包过滤防火墙就足够了。现在大部分 SOHO 路由器都具有防火墙、VPN、地址映射、端口映射、DHCP 服务、自动拨号、支持虚拟服务器以及支持动态 DNS 等功能。

华为 Quidway R1600，清华同方 TFB-104R+、Linksys、Netgear、D-Link，3Com 等公司出品的宽带路由器，WatchGuard 的 Firebox SOHO，Symantec 的 Norton Personal Firewall、NetScreen 以及 SonicWall SOHO 完全适用于这种环境；Cisco 和 Check Point 也提供小型办公室版本的 PIX 和 FireWall-1，不过价格要高一点。

2．中小型企业网络

中小型企业以及远程办公环境需要提供 Web 服务、电子邮件、流媒体以及文件传输和终端访问。防火墙较多考虑高容量、高速度、低延迟、高可靠性以及防火墙本身的健壮性，并且开始支持双机热备份。

东软 NetEye、WatchGuard Firebox 和 SonicWall 等产品比较适合这种场合。

3．大型网络

大型企业、校园网和服务提供商面对的是复杂的大型环境，拥有众多用户并提供诸多复杂服务。有些服务看似简单，但实际上需要防火墙开放多个端口服务。例如，VoIP 和 NetMeeting，这两种服务都需要为 25 种以上的不同服务开放端口。因此在复杂的大型环境中，应该使用支持集中式防火墙管理和配置功能的防火墙。例如，Cisco PIX、Check Point FireWall-1 和 NetScreen 等。

6.5 个人防火墙实例简介

6.5.1 个人防火墙

1. 个人防火墙的概念

现在网上流行的个人防火墙软件众多，功能各异。所谓个人防火墙，就是指一种能够保护个人计算机系统安全、可以直接在用户计算机操作系统上运行的软件。它是应用程序级的，使用与状态检测防火墙相同的方式来保护计算机免受攻击。通常这些防火墙安装在计算机网络接口的较低级别上，使它们可以监视通过网卡的所有网络通信。

一旦安装了个人防火墙，就可以把它设置成“学习模式”。这样，对遇到的每一种新的网络通信，个人防火墙都会提示用户一次，询问如何处理这种通信。然后，个人防火墙便记住了其响应方式，并应用于以后遇到的同种网络通信。例如，如果用户已经安装了一台个人 Web 服务器，个人防火墙可能将第一个传入的 Web 连接加上标记，并询问用户是否允许它通过。用户可能允许所有的 Web 连接、来自某些特定 IP 地址范围的连接等，个人防火墙就会将这些规则应用于此后所有传入的 Web 连接。

可以将个人防火墙想象成在用户计算机上建立的一个虚拟网络接口，此时已不再是计算机操作系统直接通过网卡进行通信，而是操作系统与个人防火墙的对话，它将仔细检查网络通信，然后再通过网卡进行通信。

2. 个人防火墙的优点

（1）增加了保护功能

个人防火墙具有安全保护功能，既可以抵挡外来攻击，也可以抵挡来自内部的攻击。例如，家庭用户使用 Modem 或 ISDN/ADSL 上网，个人防火墙就能够为用户隐藏暴露在网络上的信息（例如 IP 地址）。

（2）易于配置

个人防火墙产品通常可以使用直接的配置选项获得基本配置。

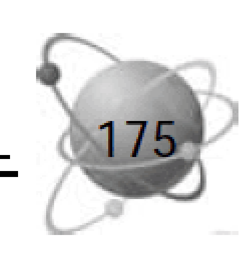
（3）廉价

个人防火墙不需要额外的硬件资源就可为内部网的个人用户和公共网络中的单个系统提供安全保护。它已被集成到 Windows XP 版本中，使用其他版本的 Windows 或其他操作系统的其他产品也可以免费获得或者按有限的成本价获得。

3. 个人防火墙的缺点

（1）接口通信受限

个人防火墙对公共网络只有一个物理接口，而真正的防火墙应当监视并控制两个或更多的网络接口之间的通信，因此个人防火墙本身可能会容易受到威胁，或者说具有网络通信可以绕过防火墙规则这样的弱点。



（2）集中管理比较困难

个人防火墙需要在每个客户端进行配置，这将增加管理开销。

（3）性能限制

个人防火墙是为了保护单个计算机系统而设计的，但是如果安装它的计算机是与内部网络上的其他计算机共享到 Internet 的连接，则它也可以保护小型网络。

个人防火墙在充当小型网络路由器时，将导致其性能下降。这种保护机制通常不如专用防火墙方案有效，因为它通常只限于阻止 IP 和端口地址。

6.5.2　瑞星个人版防火墙

相比而言，瑞星防火墙在对攻击的反应能力和反应速度方面是比较领先的，并且能够及时有效地升级和维护。目前在国内的防火墙产品中，瑞星防火墙在稳定性和防护性方面都处于领先地位，在国内得到广泛的应用。

下面就来简单了解一下这个工具。

瑞星个人防火墙是由瑞星软件公司开发的，供个人计算机使用的网络安全防护工具。它可以保护网络安全，使网络免受黑客攻击。

它采用先进的监测技术，能够有效地监控网络连接；利用内置的、细化的规则设置，使网络保护更加智能；同时，它具有游戏防盗、应用程序保护等高级功能，可为个人计算机提供全面的安全保护；并且，通过过滤不安全的网络访问服务，极大地提高了用户计算机的上网安全性，比较彻底地阻挡了黑客攻击、木马程序等网络威胁，保护上网账号、QQ 密码、网游账号等信息不被窃取。

1. 瑞星个人防火墙的安装

安装瑞星个人防火墙的具体步骤如下：

（1）下载了瑞星个人防火墙的安装程序之后，直接执行安装程序，打开其欢迎界面，如图 6-19 所示。

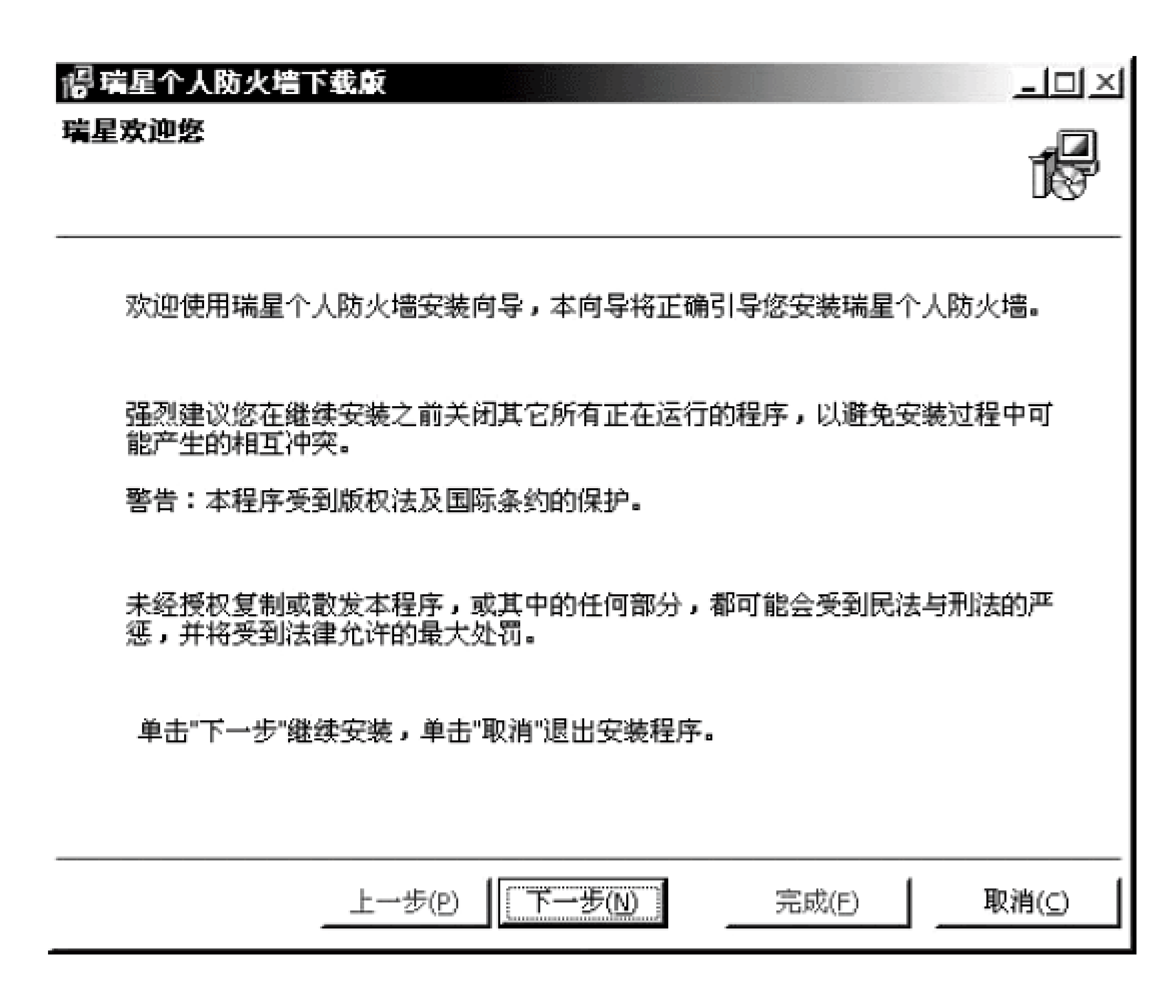


图 6-19　瑞星个人防火墙的安装欢迎界面

（2）单击“下一步”按钮，进入“最终用户许可协议”界面，要求用户阅读瑞星公司的安装协议。当然，阅读完后必须同意该条款，即选中“我接受”单选按钮，这样才可以根据安装向导继续进行软件的安装。单击“下一步”按钮，如图 6-20 所示。

（3）进入“验证产品序列号和用户 ID”界面，在“产品序列号”文本框中输入瑞星的“产品序列号”，输入后在其下面将打开“用户 ID”文本框，在此输入 12 位的用户 ID，如图 6-21 所示。

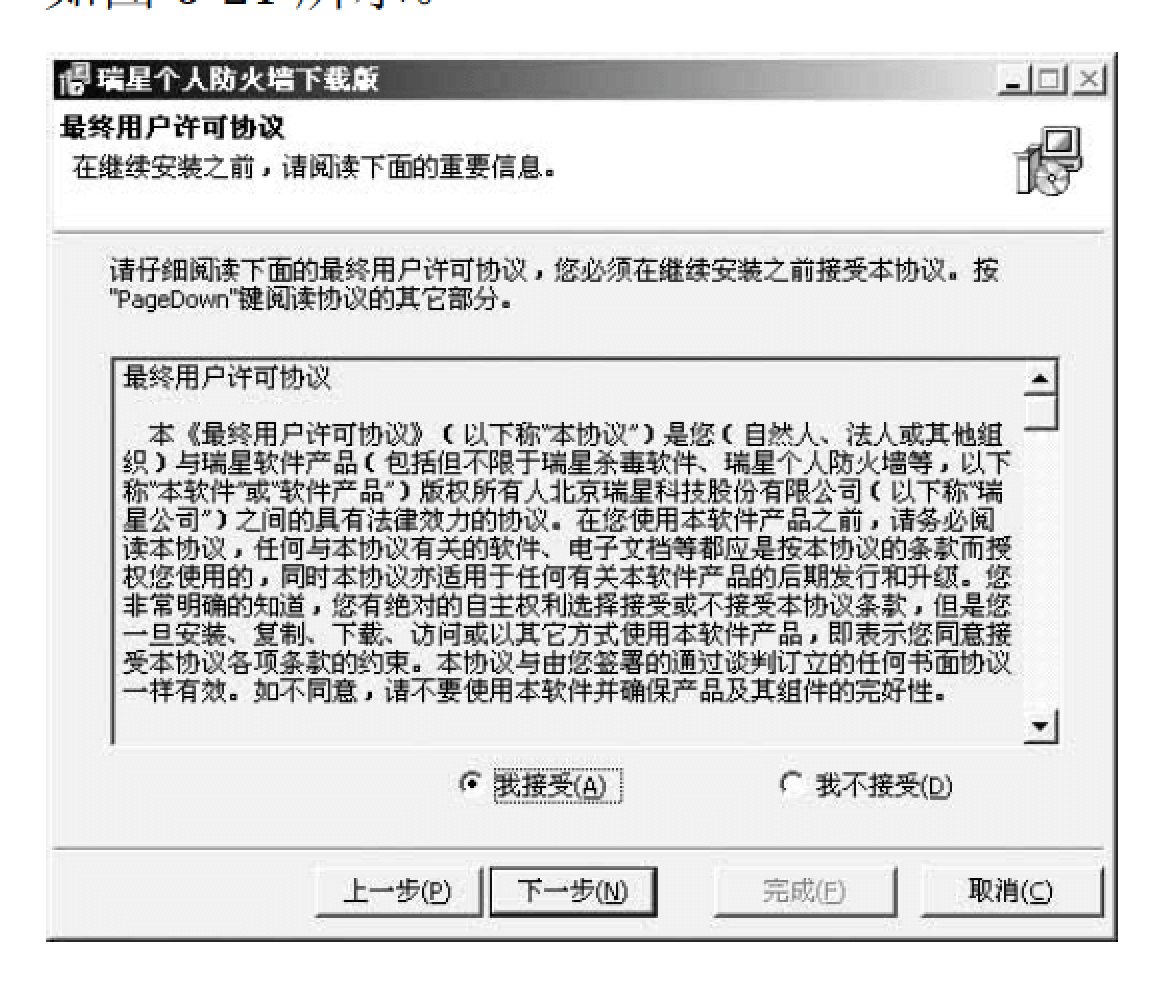


图 6-20 “最终用户许可协议”界面



图 6-21 “验证产品序列号和用户 ID”界面

（4）单击“下一步”按钮，在出现的界面中选择安装方式。瑞星个人防火墙提供了“全部安装”和“最小安装”两种安装方式。

若选择“全部安装”方式，则可以根据需要选择要安装的其他组件，例如瑞星工具、瑞星皮肤资源等，如图 6-22 所示。

（5）单击“下一步”按钮，进入“选择目标文件夹”界面，在此选择要将该软件安装到什么位置，如图 6-23 所示。一般来说，该软件的默认安装路径是 C:\Program Files\Rising\Rfw 文件夹。另外，也可以通过单击右侧的“浏览”按钮，来自行设定安装的路径。

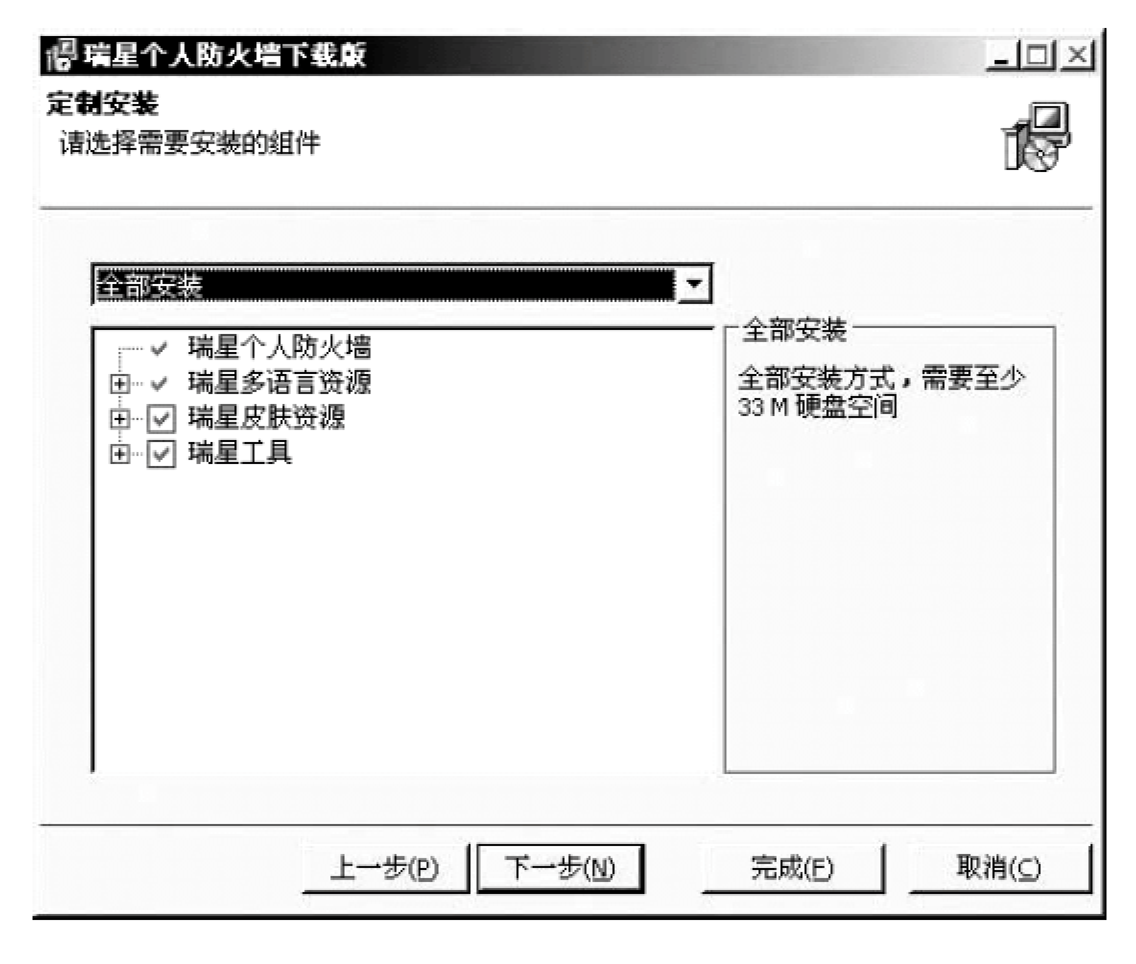


图 6-22 “定制安装”界面



图 6-23 “选择目标文件夹”界面

（6）单击“下一步”按钮，进入“选择开始菜单文件夹”界面，选择瑞星个人防火墙在系统“开始”菜单中的文件夹，以便用户可方便地通过“开始”菜单以及桌面等位置启动防火墙，如图 6-24 所示。

（7）单击“下一步”按钮，进入“安装信息”界面，其中显示了相关的安装信息，用户可最后一次检查安装信息是否正确，并确定在安装该防火墙之前是否对内存进行病毒扫描，如图 6-25 所示。

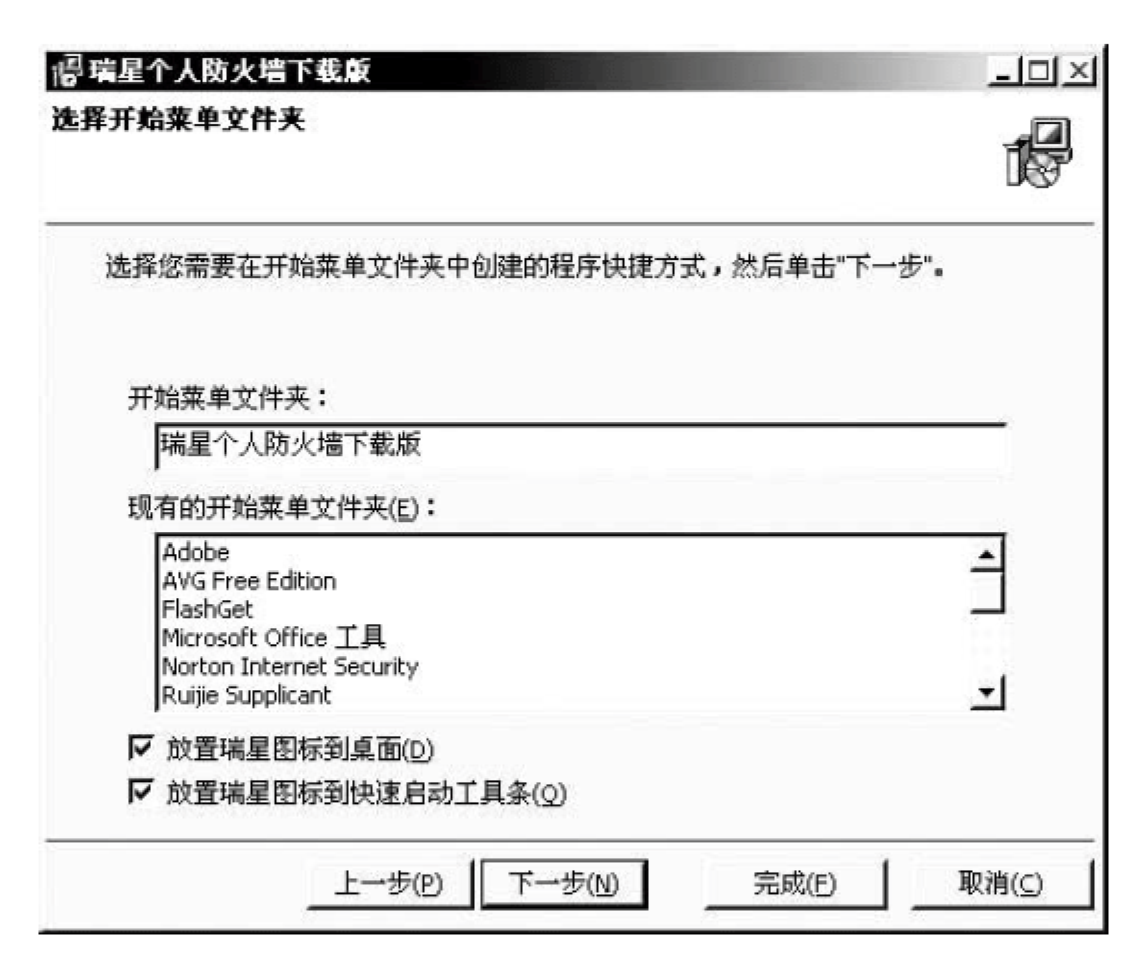


图 6-24　“选择开始菜单文件夹”界面

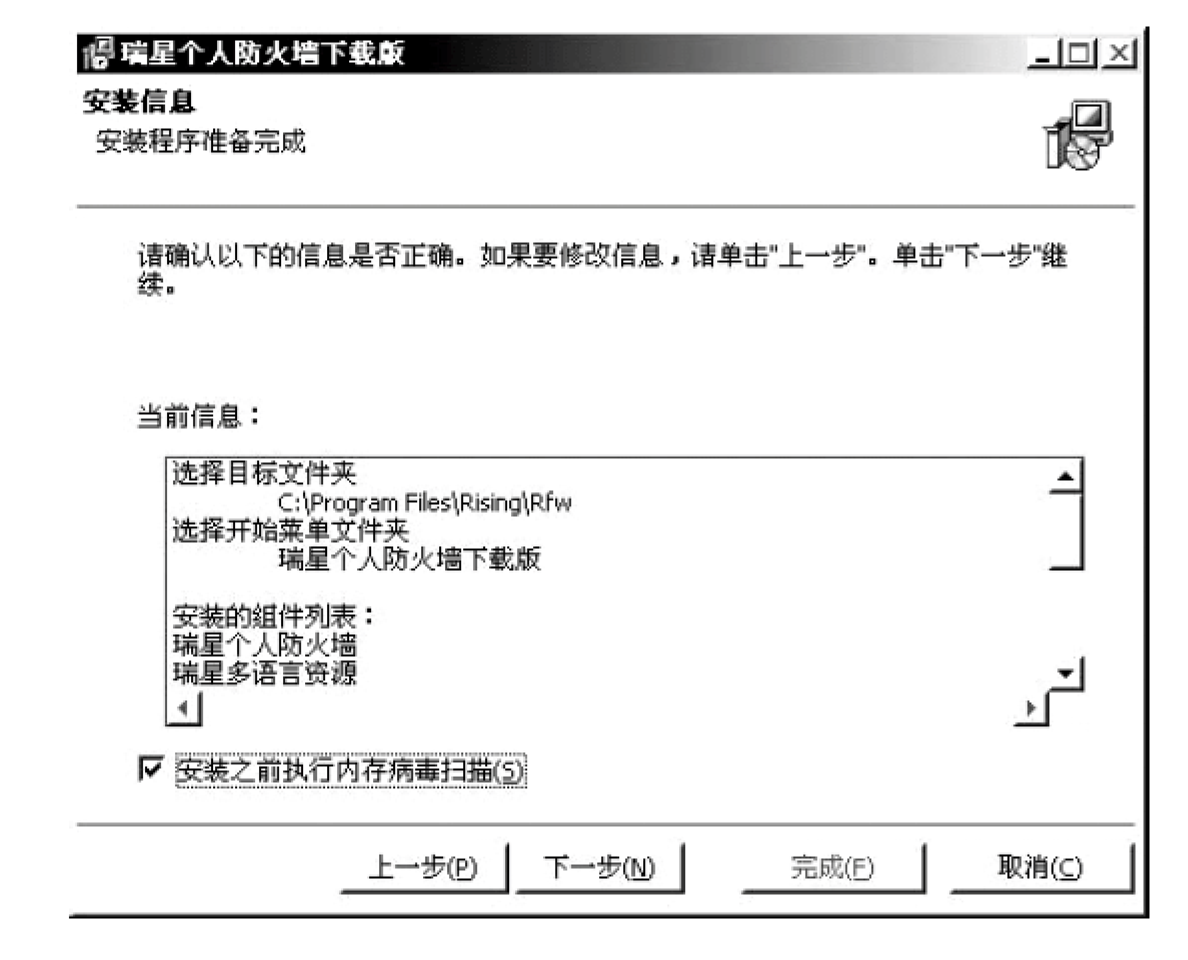


图 6-25　“安装信息”界面

（8）单击“下一步”按钮，进入“安装过程中”界面，此时将进行防火墙文件的复制和安装，如图 6-26 所示。

（9）完成瑞星个人防火墙安装后，进入“结束”界面，选中“启动瑞星个人防火墙”复选框，单击“完成”按钮，如图 6-27 所示。瑞星个人防火墙就安装到了你的计算机上。在任务栏的右侧，将会出现瑞星防火墙的图标。



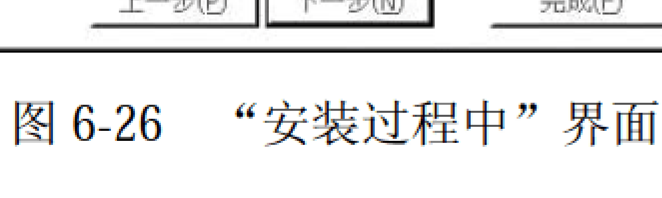

图 6-26　“安装过程中”界面



图 6-27　“结束”界面

2．瑞星个人防火墙的卸载

瑞星个人防火墙提供了自动卸载程序，卸载过程如下。

（1）单击“开始”按钮，在弹出的菜单中选择“程序”命令，找到瑞星防火墙软件的安装目录，选择“添加删除组件”命令，如图 6-28 所示。

（2）打开“瑞星软件维护模式选项”界面，选中“卸载”单选按钮，单击“下一步”按钮，如图 6-29 所示，即可完成瑞星个人防火墙的卸载。

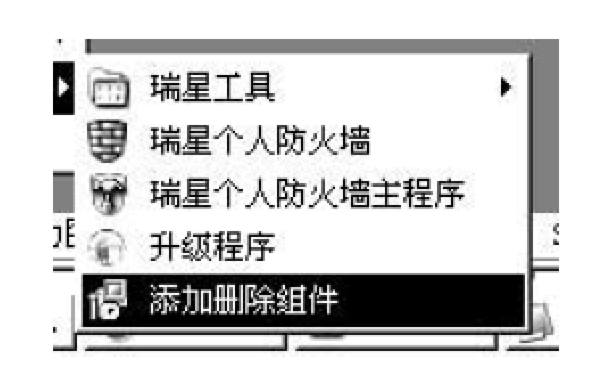


图 6-28　选择“添加删除组件”命令

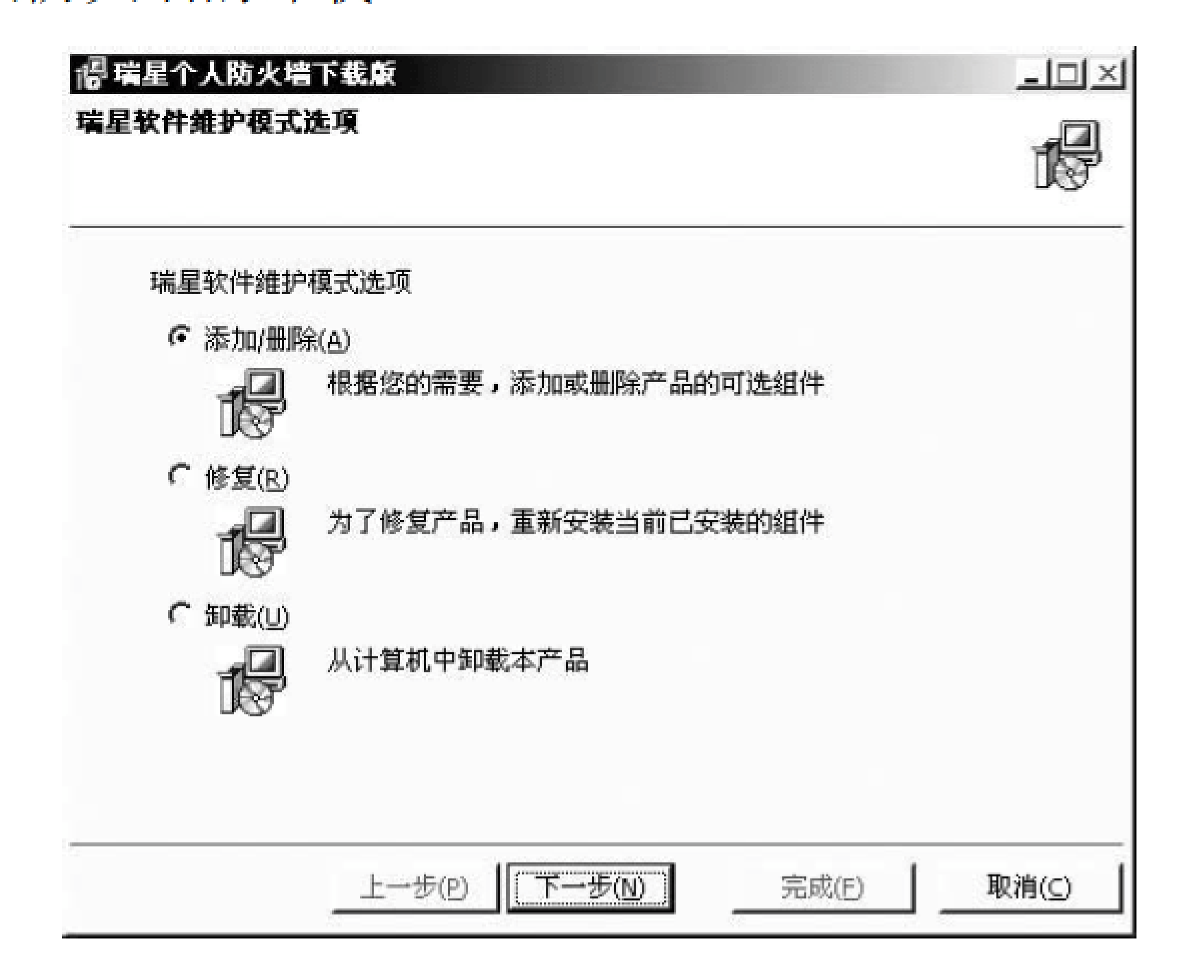


图 6-29　“瑞星软件维护模式选项”界面

当然，也可以通过控制面板中的“添加或删除程序”功能来进行卸载。

3．瑞星个人防火墙的使用与设置

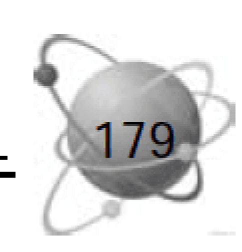
双击任务栏右下角的瑞星个人防火墙图标，打开其工作界面，如图 6-30 所示。其菜单栏中包括以下 3 个菜单项：



图 6-30　瑞星个人防火墙工作界面

（1）操作

单击该菜单项，在弹出的下拉菜单中可以看到包含有“停止保护”、“断开网络”、“切



换工作模式"、"工作日志"、"扫描木马病毒"、"智能升级"以及"退出"几个子菜单，可以实现瑞星个人防火墙的基本操作。

（2）设置

单击该菜单项，在弹出的下拉菜单中可以看到包含有"详细设置"、"密码保护"、"外观选择"、"设置网络"和"设置用户 ID"等几个子菜单。

其中，"详细设置"是配置防火墙策略的主要工具。下面将具体介绍设置的内容。

选择"详细设置"命令后，将出现如图 6-31 所示的"详细设置"对话框。

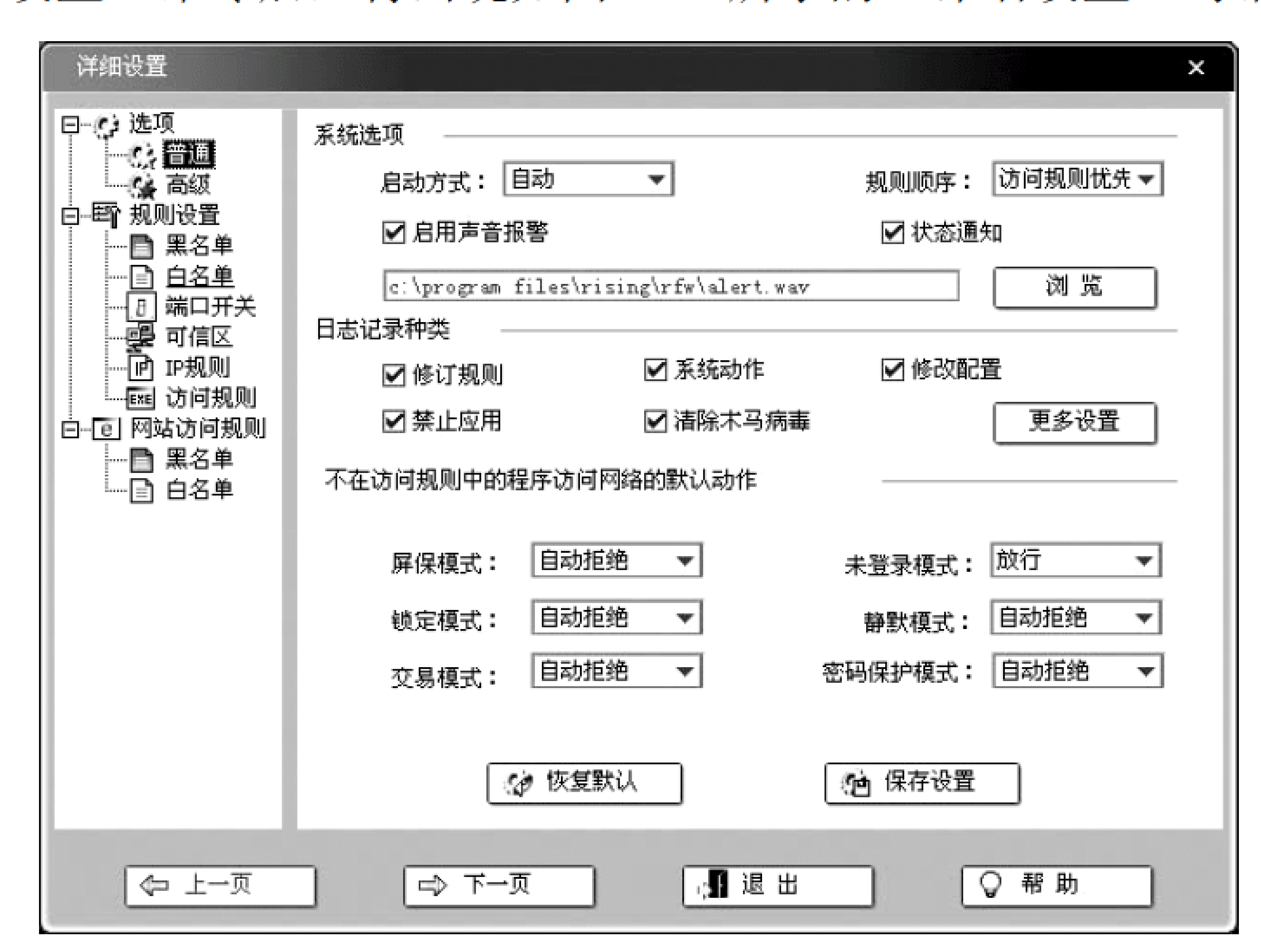


图 6-31　"详细设置"对话框

① 选项

选项共有两个可选内容，分别是"普通"选项与"高级"选项。

在"普通"选项中，可设置该系统的启动方式、匹配规则时所采用的顺序、记录哪些动作到日志中以及对不在规则中的访问所采取的默认动作。

在"高级"选项中可进一步对防火墙的安全、提示时间、漏洞扫描时间等进行设置。

② 规则设置

规则设置用来配置防火墙的过滤规则。其中包括：

- 黑名单：用于禁止该区域中的计算机与本机通信，例如曾攻击过本机的计算机可加入此区域。
- 白名单：完全信任的计算机可加入此区域，例如 VPN 服务器。
- 端口开关：可用手工控制，端口是否可以通信。
- 可信区：指定局域网计算机的 IP，默认对方计算机不在此区域中。
- IP 规则：定义在 IP 层进行过滤的规则。
- 访问规则：在本机中访问网络中程序的过滤规则。

③ 网站访问规则

用于设置监视的端口（例如端口 80、88、82），并将访问这些端口的网站加入到黑名

单或白名单中去。

（3）帮助

和其他应用程序的“帮助”菜单一样，都是为了帮助用户更好地使用瑞星个人防火墙。

4. 选项卡介绍

瑞星个人防火墙提供了 6 个不同的选项卡，方便用户了解相关的安全信息。

（1）工作状态

提供防火墙的工作状态（例如，防火墙过期了，就会在系统状态栏中显示），并在此显示相关的受攻击信息、当前的活动程序、系统存在的漏洞和不安全设置等提示。

（2）系统状态

显示当前系统所监视的程序。

（3）启动选项

用于显示系统启动和登录时自动运行程序的信息，这些程序可能是系统启动菜单中的程序、注册表中的 Run、RunOnce 和其他的一些键值。

如果在下次启动时不想运行某些程序，可以禁止或删除这些程序。

（4）密码保护

受保护的一些程序被其他的应用程序访问时，将被禁止。

若要允许信任的模块访问被保护进程，需要将指定模块添加到信任模块列表中去。

其规则和信任模块等，都在该选项卡中设定。

（5）漏洞扫描

扫描，并将发现的安全漏洞等信息以报告的形式显现出来。

（6）安全资讯

列出当前整个互联网中新的安全动态，以及瑞星公司的最新安全举措。

5. 瑞星个人防火墙的升级

随着网络环境的不断变化，任何网络安全产品要实现对系统的保护，就必须定期升级。

可以直接单击工作界面中的“智能升级”按钮，或选择“操作”/“智能升级”命令，来对瑞星个人防火墙进行升级。在升级过程中，将自动对瑞星个人防火墙进行最新版本的搜索，出现如图 6-32 所示的升级界面，直至升级完成。

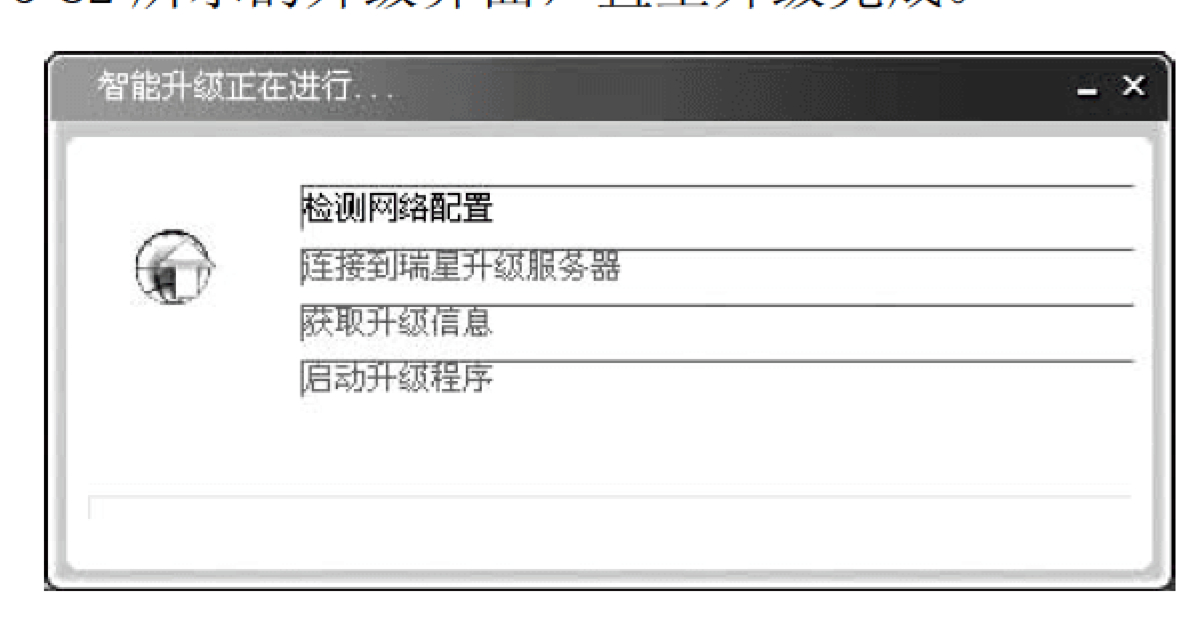


图 6-32 瑞星个人防火墙升级界面

小　结

防火墙通常是指设置在不同网络（例如可信任的内部网络和不可信任的外部网络）或网络安全域之间的一系列部件的组合。它是一种必不可少的安全增长点，是设置在被保护网络和外部网络之间的一道屏障，也是不同网络或网络安全域之间信息的唯一出入口，能根据网络安全策略控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础和核心控制设备，能够有效地监控内部网和互联网之间的任何活动，防止发生不可预测的、潜在破坏性的侵入，从而保证内部网络的安全。

防火墙的功能主要体现在：它是网络安全的屏障、可以强化网络安全策略、对网络存取和访问进行监控审计以及防止内部信息的外泄 4 方面。

防火墙也有其局限性，它不是解决所有网络安全问题的万能药方，而只是网络安全策略中的一个组成部分。

防火墙有多种不同的分类方法：根据采用的技术不同，可分为包过滤防火墙和代理服务器防火墙；按照应用对象的不同，可分为企业级防火墙与个人防火墙；依据实现的方法不同，又可分为软件防火墙、硬件防火墙和专用防火墙。

包过滤是防火墙为系统提供安全保障的主要技术，它依据系统内设置的访问控制表，在网络层对进出网络的数据包进行有选择的控制与操作。包过滤操作一般都是在选择路由的同时，在网络层对数据包进行选择或过滤。

包过滤防火墙逻辑简单、价格便宜、易于安装和使用、网络性能和透明性好，通常安装在路由器上，而路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

包过滤的缺点是安全性较差、一些应用协议不适用包过滤防火墙、正常的数据包过滤路由器无法执行某些安全策略、不能彻底防止地址欺骗和数据包工具存在很多局限性等。

代理服务器是运行在防火墙主机上的一些特定的应用程序或者服务程序，它们代表客户在服务器端进行连接请求。当代理服务器收到一个客户的连接请求时，它将核实客户请求，并用特定的安全化的代理应用程序来处理连接请求，并将处理后的请求传递到真实的服务器上，然后接收服务器应答，并作进一步处理后，将答复交给发出请求的最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接和隔离内、外部网络的作用，所以又称为代理防火墙。

代理防火墙分为应用层网关和电路级网关两类。

应用层网关防火墙是传统代理型防火墙，在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时对数据包进行必要的分析、登记和统计，形成报告。

应用层网关防火墙最突出的优点就是安全，最大缺点就是速度相对比较慢。

电路级网关是建立应用层网关的一种更加灵活的方法，是针对包过滤和应用层网关技术存在的缺点而引入的防火墙技术。电路级网关通过在 TCP 3 次握手建立连接的过程中，检查双方的 SYN、ASK 和序列号是否符合逻辑，来判断该请求的会话是否合法。一旦网关认为会话是合法的，就为双方建立连接，并维护一张合法会话连接表，当会话信息与表中的条目匹配时才允许数据通过，会话结束后，表中的条目就被删除。

代理技术具有代理易于配置、代理能生成各项记录、代理能灵活并且完全地控制进出流量和内容、代理能过滤数据内容、代理能为用户提供透明的加密机制、代理可以方便地与其他安全手段集成等优点。

代理技术具有代理速度较路由器慢、代理对用户不透明、对于每项服务代理可能要求不同的服务器、代理服务不能保证免受所有协议弱点的限制和代理不能改进底层协议的安全性等缺点。

单纯的包过滤技术简单地查看每一个单一的输入包信息，而状态包检测模式则增加了更多的包和包之间的安全上下文检查，以达到与应用级代理防火墙相类似的安全性能。状态包检测防火墙在网络层拦截输入包，并利用足够的企图连接的状态信息作出决策。

自适应代理技术是较新的一种防火墙设计，它将代理服务技术和状态包检测技术结合在一起。其基本的安全检测仍在应用层进行，但一旦安全检测代理明确了会话的所有细节，那么其后的数据包就可以直接经过速度更快的网络层。因此，自适应代理防火墙基本上和标准代理服务防火墙一样安全，并且比状态包检测有更快的性能。

目前，防火墙的体系结构一般有屏蔽路由器体系结构、双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构 4 种。

屏蔽路由器是最简单也是最常见的防火墙，它除了具有路由功能外，可安装包过滤软件，利用包过滤规则完成基本的防火墙功能。

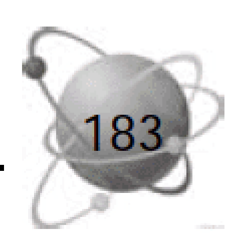
双重宿主主机体系结构是围绕具有双重宿主的堡垒主机构筑的，它分别连接到因特网和内部网络，并且位于两者之间。防火墙内部的系统能与双重宿主主机通信，同时防火墙外部的系统（在因特网上）也能与双重宿主主机通信，但是这些系统之间不能直接互相通信，它们之间的 IP 通信被完全阻止。

屏蔽主机网关由屏蔽路由器和应用网关组成，屏蔽路由器的作用是包过滤，应用网关的作用是代理服务，即在内部网络和外部网络之间建立了两道安全屏障，既实现了网络层安全（包过滤），又实现了应用层安全（代理服务）。

屏蔽子网防火墙是在屏蔽主机网关防火墙的基础上再加一个路由器，两个屏蔽路由器放在子网的两端，形成一个隔离区。内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网进行通信。

搭建防火墙时，一般很少采用单一的技术，通常采用解决不同问题的多种技术的组合。例如，采用多堡垒主机、合并内部路由器和外部路由器、合并堡垒主机和外部路由器、合并堡垒主机和内部路由器、使用多台外部路由器、使用多个周边网络等组合体系结构。

选购防火墙产品时，用户首先需要了解一个防火墙系统应具备的基本功能；其次，选购防火墙的时候主要应该考虑安全性、高效性、适用性、可管理性和售后服务体系等因素。

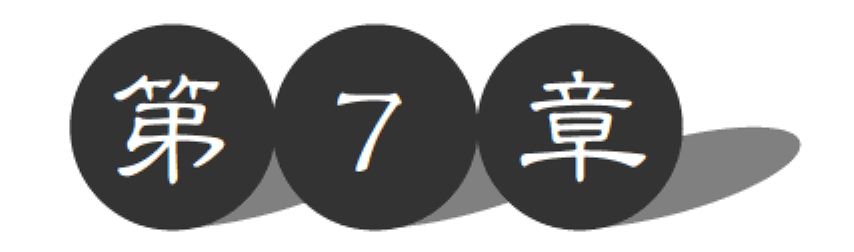


个人防火墙是一种能够保护个人计算机系统安全、可以直接在用户计算机操作系统上运行的软件。它使用与状态检测防火墙相同的方式，来保护计算机免受攻击。通常这些防火墙安装在计算机网络接口的较低级别上，使它们可以监视通过网卡的所有网络通信。

个人防火墙具有增加了保护功能、易于配置和廉价等优点，而接口通信受限、集中管理比较困难和性能限制是其主要缺点。

练习与思考

1．什么是防火墙？简述防火墙工作原理。
2．简述防火墙的发展历史。
3．设置防火墙的目的是什么？防火墙的局限性是什么？
4．简述防火墙的发展动态和趋势。
5．防火墙的主要技术及实现方式有哪些？
6．试述包过滤防火墙的原理、特点及其优、缺点。
7．试述代理防火墙的原理及特点。应用层网关和电路级网关有什么区别？
8．试比较包过滤防火墙和代理防火墙的不同之处。
9．试述状态检测和自适应代理防火墙的原理及特点。
10．防火墙的体系结构有哪些？试述各种防火墙体系结构的优缺点。
11．屏蔽路由器的优缺点是什么？为什么堡垒主机不能有 IP 转发功能？
12．屏蔽路由器防火墙和屏蔽主机防火墙各是如何实现的？
13．组合体系结构都有哪些形式？
14．防火墙产品的选购策略有哪些？
15．Check Point FireWall-1 可以提供什么基本模块？它成功的部分原因是什么？
16．Cisco PIX Firewall 的特点是什么？
17．个人防火墙有什么特点？



第7章 计算机病毒防治

本章学习要求：

（1）了解计算机病毒的基本概念、发展、特点、分类、危害。
（2）掌握计算机病毒的工作机理。
（3）了解恶意代码的分类及其特点。
（4）了解木马的基本概念、特点、工作过程、危害。
（5）掌握木马的检测和清除以及预防方法。
（6）了解蠕虫的基本概念、分类、特点、危害。
（7）掌握蠕虫的基本结构、传播方式及其防范措施。
（8）熟悉计算机病毒的传播途径和防治管理措施。
（9）了解预防计算机病毒应注意的问题。
（10）掌握计算机病毒的检测和清除方法。
（11）熟悉常用计算机病毒防治软件的名称及其特点。
（12）掌握瑞星杀毒软件的安装、卸载、菜单功能、使用和升级方法。
（13）掌握计算机网络病毒、宏病毒的检测和清除方法。
（14）了解计算机病毒的现状和发展趋势。

重点和难点：

（1）重点：计算机病毒的工作机理；木马的检测和清除以及预防方法；蠕虫的基本结构、传播方式及其防范措施；计算机病毒的检测和清除方法；瑞星杀毒软件的安装、卸载、菜单功能、使用和升级方法；计算机网络病毒、宏病毒的检测和清除方法。

（2）难点：计算机病毒的检测和清除方法；计算机网络病毒、宏病毒的检测和清除方法。

相信大家对计算机病毒都不会感到陌生，凡是用过计算机的人，几乎都和它打过交道，而其中被计算机病毒搞得焦头烂额，对其恨之入骨的人也不在少数。这也从一个侧面说明

计算机病毒的危害之深，作恶范围之广。对计算机病毒的防治一直是有关专家的研究课题，但在计算机病毒与防治病毒的战争中，正义的一方并没有占据明显的优势。

计算机病毒对安全的危害随着互联网的发展而逐渐升级。在以前的主机时代，由于计算机独立工作，当时的数据共享主要是通过软盘进行，因此病毒的传播也局限在很小的范围内；而且病毒防治工作也很简单，只要密切注意软盘复制即可。然而到了网络时代，随着 Internet 的普及，越来越多的计算机连接到互联网上，计算机病毒制造者开始将互联网作为计算机病毒的主要传播载体。前几年的“冲击波”和“震荡波”病毒充分利用了互联网的特点，在短短几天之内就造成了全球范围的病毒事件。

因此，互联网的发展给计算机病毒防治工作带来了很大的难度。但是任何事情都有两面性，互联网也成为了防病毒厂商、安全团体及时发布消息的主要途径，而且绝大多数防病毒软件都可以通过互联网对病毒库和防病毒程序进行在线升级。

随着计算机病毒的危害性日益被人们所认识，以及病毒研制技术的不断提高，计算机病毒已被越来越多地应用于特殊目的。例如，某些组织或个人将其用于军事目的，通过预先在敌方的指挥或控制系统中植入病毒，达到扰乱和破坏的目的。有专家认为，随着人们对计算机和网络的依赖程度越来越高，计算机病毒可能成为恐怖分子实施恐怖袭击的有力工具。

本章将从计算机病毒的概念、发展、危害及其特点等方面谈起，介绍计算机病毒的分类，并结合具体的例子介绍恶意代码、计算机病毒尤其是典型计算机病毒的检测与清除。最后，简单回顾计算机病毒的现状和发展趋势。

7.1　计算机病毒的特点与分类

7.1.1　计算机病毒的概念

从广义上讲，凡是能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。依据此定义，诸如“逻辑炸弹”、“蠕虫”等均可称为计算机病毒。在国内，专家和研究者们曾对计算机病毒作过多种不尽相同的定义，但一直没有公认的明确定义。

最早使用“计算机病毒”一词的美国计算机病毒研究专家 F.Cohen 博士对计算机病毒的定义是：计算机病毒是一种能够通过修改程序，并把自己的复制品包括在内去感染其他程序的程序。或者说：计算机病毒是一种在计算机系统运行过程中能把自己精确复制或有修改地复制到其他程序体中的程序。

1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用并能自我复制的一组计算机指令或者程序代码。”此定义具有法律效力和权威性。

“计算机病毒”这一名词来源于它们的生物学同类，它具有与生物病毒相似的行为特

性。计算机病毒能够在计算机内部反复地自我繁殖和扩散，危及计算机系统或网络的正常工作，造成种种不良后果，最终可能使计算机系统或网络发生故障以至瘫痪。这种现象与生物界病毒在生物体内部繁殖，相互传染，最终引起生物体致病甚至死亡的过程极为类似，所以人们把它形象地称为“计算机病毒”。

计算机病毒赖以生存的基础是现代计算机都具有相同的工作原理和操作系统的脆弱性，以及网络协议中的安全漏洞。特别是在个人计算机中，系统的基本控制功能对用户是公开的，可以通过调用和修改系统的中断，取得对系统的控制权，从而对系统程序和其他程序进行任意处理。正是在此基础上，一些计算机专业人员出于开玩笑、炫耀技术水平和惩罚复制等原因，研制了一些病毒程序，从而使病毒程序不断蔓延，所造成的后果恐怕也是这些人当初始料不及的。

7.1.2 计算机病毒的发展

计算机病毒是伴随着计算机的发展而不断发展变化的。

对计算机病毒的讨论开始于 20 世纪 40 年代，当时已有人注意到程序可以编制成自我复制并增加自身大小的形式，但这些讨论只是理论性的。

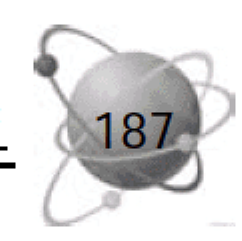
50 年代，美国电报电话公司贝尔实验室的一些科学家开始用一种称为“核心大战（Core War）”的计算机代码游戏进行实验。这群年轻的研究人员常常在做完工作后留在实验室里饶有兴趣地玩一种他们自己创造的计算机游戏——“达尔文”，即每个人编写一段小程序，输入到计算机中运行，互相展开攻击并设法毁灭他人的程序。这种程序就是计算机病毒的雏形，然而当时人们并没有意识到这一点。

60 年代，有人开发了一种称为“生存（Living）”的软件，它可以进行自我复制。由此创造病毒类程序的挑战开始在学术、研究界流行开来，但这些病毒的作者通常只是用它们开一些无关痛痒的小玩笑。

70 年代，计算机黑客们对这类程序的研究有了很大的进展，但很少有真正的病毒攻击报道。1975 年，美国科普作家 John Bruner 在他名为《震荡波骑士》（Shockwave Rider）的科幻小说中，第一次使用了“计算机病毒”这个名词。

80 年代，随着 PC 机的日益普及，病毒对计算机系统的巨大威胁开始出现在公众面前。真正意义上的“计算机病毒”出现于 1981 年，病毒 Elk Cloner 驻留在磁盘的引导扇区上，通过磁盘进行感染。由于该病毒只是关掉显示器，让显示的文本闪烁或显示一大堆无意义的信息，并没有造成较大的破坏，所以当时没有引起足够的关注。

最早被记录下来的病毒之一是美国南加州大学的学生 Fred Cohen 于 1983 年编写的。当该程序安装到硬盘之后，就可以对自己进行复制和扩展，使计算机“自我破坏”。同年 11 月 3 日召开的计算机安全学术讨论会上，美国计算机安全专家科恩（Frederick Cohen）博士首次提出了“计算机病毒”的概念，随后获准进行实验演示。专家们在运行 UNIX 操作系统的 VAX11/750 计算机系统上进行了 5 次病毒试验，结果表明病毒平均 30 分钟就可使计算机系统瘫痪，从而确认了计算机病毒的存在，使人们认识到了计算机病毒对计算机



系统的破坏作用。

1986 年底，由巴基斯坦两兄弟 Basit 和 Amjad Farooq A1vi 制造的病毒 Brain 开始流行。为迷惑计算机用户，Brain 病毒首次使用了伪装手段。Brain 的蔓延引起了新闻媒体的注意，美国新闻机构于 1987 年 10 月报道了这一例计算机遭病毒入侵及引起破坏的事件，从此计算机病毒开始受到广大民众的关注。

从 20 世纪 90 年代至 21 世纪初，几乎年年都会出现新的病毒品种，其影响的范围越来越广，对计算机的硬件和软件的破坏性也越来越严重。由于篇幅的限制，就不在此一一列举了，对病毒有兴趣的读者可查阅相关资料。

2004 年，为对抗防病毒工具的追杀，实现更大范围的传播，计算机病毒开始频繁地变种。例如，“网络天空”病毒（I-Worm/NetSky）、“雏鹰”病毒（I-Worm/BBEagle），一经发现就已有数十个变种，在病毒排行榜中长期居高不下。同时，窃取银行账号、信用卡、游戏账号、邮箱账号等偷窃个人信息性质的木马病毒数量增长迅速。同年 4 月，云南一网吧 80 余台计算机的网络游戏账号一夜之间全部被盗。

紧接着出现了“网银大盗”病毒，它能够轻松绕过某银行网上银行系统的安全插件，盗窃用户银行卡账号及密码。随后，在人们庆幸“网银大盗”作者落网的同时，其他病毒、木马开始泛滥，层出不穷。例如，“网银大盗 II”木马病毒惊现网络，几乎所有网上银行的用户成为病毒侵害的目标；“证券大盗”木马病毒（Trojan/PSW.Soufan）则可以盗取多家证券交易系统的交易账号和密码，被盗号的股民账户存在着被人恶意操纵的可能性；“蜜蜂大盗”病毒具有强大的信息窃取、远程监控功能，可以窃取几乎所有类型的密码，自动打开染毒者的摄像头，进行远程监控、远程摄像、遥控 QQ，并可中止防火墙；而“黑洞”病毒不但能够像“蜜蜂大盗”那样自动开启用户的摄像头偷窥隐私，盗取用户所有密码，掌控用户计算机中的所有资料，而且还具有录音功能，能够偷录下用户语音、视频聊天的一切隐私。

随着计算机软硬件的发展和网络技术的普及，计算机病毒的编制技术也在不断地适应新的变化，采用新的技术，扩展新的领域。病毒和防病毒必将长期并存、斗争不已。

总之，从 1986 年出现第一个感染 PC 机的计算机病毒开始，至今短短 30 年，已经经历了 3 个阶段。第一个阶段为 DOS、Windows 等传统病毒，此时编写病毒完全是基于对技术的探求，这一阶段的顶峰应该算是 CIH 病毒；第二个阶段为基于 Internet 的网络病毒，例如“红色代码”、“冲击波”、“震荡波”等病毒皆属于此阶段，这类病毒往往利用系统漏洞进行世界范围内的大规模传播；目前计算机病毒已经发展到了第三阶段，我们所面临的不再是一个简简单单的病毒，而是集病毒、黑客攻击、木马、间谍软件等多种危害于一身的基于 Internet 的网络威胁。

7.1.3　计算机病毒的特点

1．发生侵害的主动性

病毒程序的目的就是为了侵害他人的计算机系统或网络系统。在计算机系统的运行过

程中，病毒始终以功能过程的主体出现，而形式则可能是直接或间接的。病毒的侵害方式代表了设计者的意图，因此病毒对计算机运行控制权的争夺、对其他程序的侵入、传染和危害，都采取了积极主动的方式。

2．传染性

这是病毒的基本特征。

病毒的设计者总是希望病毒能够在较大的范围内实现蔓延和传播，感染更多的程序、计算机系统或计算机网络系统，以达到最大的侵害目的。

病毒是人为设计的功能程序，所以它必须利用一切可能的途径和方法进行传染。程序之间的传染通常是由病毒的传染模块执行的，它借助于正常的信息处理途径和方法，例如磁盘的引导、启动、程序的调用、存储器的驻留，以及程序代码的增加、删除、修改等；而计算机系统之间的病毒传播通常是通过软盘、光盘等信息载体和网络通信等信息传输途径进行。具体地讲，计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。它会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。

是否具有传染性，是判别一个程序是否为计算机病毒的最重要条件。

3．隐蔽性

设计病毒的动机就是要对计算机系统进行非授权的非法活动，对计算机系统进行侵害。清除病毒是广大计算机用户的一致要求。在侵害和反侵害的对抗中，计算机病毒常常会借助于各种技巧来隐藏自己的行踪，保护自己，从而做到在被发现及清除之前，能够在更广泛的范围内进行传染和传播，期待发作时可以造成更大的破坏性。

计算机病毒都是一些可以直接或间接运行的具有较高超技巧的程序，它们可以隐藏在操作系统中，也可以隐藏在可执行文件或数据文件中，目的是不让用户发现它的存在。常用的隐藏方法有贴附、取代、隐藏在磁盘的非规范区域的缝隙中、驻留在内存的坏簇中、变异或衍生、加密和反跟踪等。

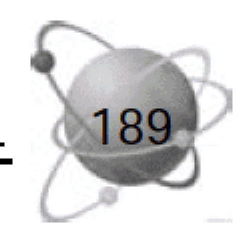
如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。一般在没有防护措施的情况下，受到感染的计算机系统通常仍能正常运行，用户不会感到任何异常。大部分的病毒代码之所以设计得非常短小，也是为了隐藏。病毒一般只有几百或一千字节。

4．表现性

病毒一旦被启动，就会立刻开始进行破坏活动。为了能够在合适的时机开始工作，必须预先设置触发条件并且首先将其设置为不触发状态。最典型的触发方式是那种基于某个特定日期的，例如星期五同时又是 13 号或 3 月 6 日（米开朗基罗的生日）。其他的触发方式可以更巧妙，例如当程序运行了多少次之后，或者当某个计算机系统被同一种病毒感染了多少次之后，或者某个特定的用户标识符或文件名或文件扩展名的出现或使用等。

5．破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响，轻者会降低计



算机工作效率，占用系统资源，重者可导致系统崩溃。

表现和破坏，是病毒的最终目的。

6. 难确定性

从本质上讲，病毒程序的每一条具体指令的语句和语法都是规范的，是系统所支持的，因此仅仅从程序的语句和语法是不能判断哪个程序是合法的，哪个程序是非法的。

对病毒程序的行为进行分析，病毒程序也是难以确定的。例如，病毒程序作为用户程序的子程序调用，怎么判断这种调用行为是非法的呢？如果从最终结果的有害性或无害性进行判断，则问题将转化为合法的语句+合法的语法=有益的行为效果吗？

例如，正常文件操作的增加、删除、修改和显示功能，和病毒程序进行破坏的增加、删除、修改和显示行为，是无法从增加、删除、修改和显示行为本身上进行区分的。从程序的再生和复制的角度来看，传染和复制是完全一致的。例如，一个编译自身新版本的编译程序就是合法的。所以，从行为的角度来确定某个程序是否为病毒程序也是很困难的。

7.1.4 计算机病毒的分类

为了更好地认识计算机病毒，下面按不同的方式对病毒进行分类。

1. 按其破坏性

可分为：良性病毒和恶性病毒。

（1）良性病毒。这类病毒表现较为温和，它仅仅是为了表现自己的存在。例如，显示信息、奏乐、发出声响，对源程序不做修改，也不直接破坏计算机的软硬件，对系统危害较小。但由于要进行自我复制和传染，所以会消耗系统的资源。

（2）恶性病毒。恶性病毒会对计算机的软件或硬件进行恶意攻击，使系统遭到不同程度的破坏。例如，破坏数据、删除文件、加密磁盘、格式化磁盘、破坏主板导致死机或网络瘫痪等。

2. 按其传染途径

可分为：驻留内存型病毒和非驻留内存型病毒。

（1）驻留内存型病毒。驻留内存型病毒感染计算机后，会把自身的内存驻留部分放在内存中，始终处于激活状态，一直到关机或重新启动。

（2）非驻留内存型病毒。非驻留内存型病毒在得到机会激活时，并不感染计算机内存。另有一些病毒在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被划分为非驻留内存型病毒。

3. 按连接方式

可分为：源码型、入侵型、操作系统型和外壳型病毒。

（1）源码型病毒。源码型病毒较为少见，亦难编写、传播。因为它要攻击高级语言编写的源程序，在源程序编译之前插入其中，并随源程序一起编译、连接成可执行文件。这

样，刚刚生成的可执行文件便已经带毒了。

（2）入侵型病毒。入侵型病毒可用自身代替正常程序中的部分模块或堆栈区，因此这类病毒只攻击某些特定程序，针对性强。一般情况下，也难以发现和清除。

（3）操作系统型病毒。操作系统型病毒可用其自身部分加入或替代操作系统的部分功能。因其直接感染操作系统，这类病毒的危害性也较大。

（4）外壳型病毒。外壳型病毒将自身附在正常程序的开头或结尾，相当于给正常程序加了个外壳。大部分的文件型病毒都属于这一类。

4. 按寄生方式

可分为：引导型病毒、文件型病毒以及集两种病毒特性于一体的复合型病毒和宏病毒、网络病毒。

（1）引导型病毒。引导型病毒会改写（即一般所说的“感染”）磁盘上的引导扇区或硬盘上分区表的内容。如果用已感染病毒的软盘来启动系统的话，则会感染硬盘。

（2）文件型病毒。文件型病毒主要以感染文件扩展名为.com、.exe 和.ovl 等可执行程序为主。它的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，方能把文件型病毒引入内存。感染此病毒的文件执行速度会减缓，甚至完全无法执行。有些文件遭感染后，一执行就会遭到删除。

（3）复合型病毒。复合型病毒综合了引导型和文件型病毒的特性，其“性情”也就比引导型和文件型病毒更为“凶残”。此种病毒通过上述两种方式来感染，更增加了病毒的传染性以及存活率。不管以哪种方式传染，只要中毒就会经开机或执行程序而感染其他的磁盘或文件。此种病毒也是最难杀灭的。

（4）宏病毒。宏病毒一般是指寄存在 Microsoft Office 文档上的病毒宏代码。它影响对文档的各种操作，如打开、存储、关闭或清除等。当打开 Office 文档时，宏病毒程序就会被执行，即宏病毒处于活动状态，当触发条件满足时，宏病毒才开始传染、表现和破坏。

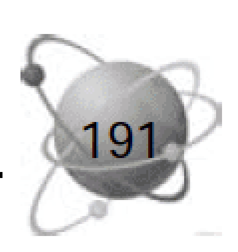
（5）网络病毒。网络病毒大体上可分为两类：一类是局域网上的病毒；另一类就是随着互联网的兴起而产生的新的网络病毒。

网络病毒又可以根据提供的服务来进一步细分。互联网提供了众多的服务，例如 WWW 服务、电子邮件服务、文件传输服务等。病毒可以利用这些服务来传播，因而可以把网络病毒分为邮件病毒、网页病毒、FTP 病毒等。其中，邮件病毒在网络病毒中占了绝大多数。

网络病毒最显著的特征是其传播过程与传统单机病毒截然不同，网络病毒的传播无须普通用户的介入。网络病毒侵入网络后，将自动收集有用信息，例如电子邮件地址列表、网络中传输的明文口令等，或者是自动探测其他计算机上存在的漏洞，然后据此向网络中的其他计算机传播。

5. 其他一些分类方式

按照计算机病毒攻击的操作系统，可将病毒分为攻击 DOS 系统的病毒、攻击 Windows 系统的病毒、攻击 UNIX 系统的病毒、攻击 OS/2 系统的病毒；按照计算机病毒激活的时间，可分为仅在某一特定的时间才发作的定时病毒和不由时钟来激活的随机病毒；按计算机病



毒攻击的机型，还可将病毒分为攻击微型机的病毒、攻击小型机的病毒和攻击工作站的病毒。

7.1.5　计算机病毒的危害

计算机病毒的主要危害有：

1．病毒激发对计算机数据信息的直接破坏作用

大部分病毒在激发的时候会直接破坏计算机系统的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的“垃圾”数据改写文件、破坏 CMOS 设置等。

例如，“磁盘杀手”病毒内含计数器，在硬盘染毒后累计开机时间达到 48 小时即会激发。激发的时候，屏幕上显示 Warning!! Don’t turn off power or remove diskette while Disk Killer is Processing!（警告！D1SK KILLER 正在工作，不要关闭电源或取出磁盘）。

提示：被 D1SK KILLER 破坏的硬盘可以用杀毒软件修复，不要轻易放弃。

2．占用磁盘空间

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。

引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区，而把原来的引导扇区转移到其他扇区，也就是引导型病毒要覆盖一个磁盘扇区，被覆盖扇区的数据将永久性丢失，无法恢复。

文件型病毒利用一些 DOS 功能进行传染，这些 DOS 功能能够检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用部位去，所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间。一些文件型病毒的传染速度很快，在短时间内可感染大量文件，每个文件都不同程度地被加长了，从而造成磁盘空间的严重浪费。

3．抢占系统资源

除 VIENNA、CASPER 等少数病毒外，其他大多数病毒在动态时都是常驻内存的，这就必然抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当。病毒抢占内存，将导致内存减少，一部分软件不能运行。

除占用内存外，病毒还会抢占中断，干扰系统运行。病毒为了传染、激发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰系统的正常运行。

4．影响计算机的运行速度

病毒进驻内存后，不但干扰系统运行，还会影响计算机的运行速度。主要表现在：

（1）病毒为了判断传染、激发条件，总要对计算机的工作状态进行监视。

（2）有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且使进驻内存后的动态病毒也处在加密状态。CPU 每次寻址到病毒处时，要运行一段解密程序把加密的病毒解

密成合法的 CPU 指令再执行；而病毒运行结束时，再用一段程序对病毒重新加密。这样，CPU 额外执行了数千条以至上万条指令。

（3）病毒在进行传染时，同样要插入非法的额外操作。特别是传染软盘时，不但计算机的速度明显变慢，而且软盘正常的读写顺序会被打乱，发出刺耳的噪声。

7.1.6 计算机病毒的工作机理

1. 计算机病毒的结构

了解病毒的编制技术，才能更好地防治和清除病毒。要想了解计算机病毒的工作机理，首先要了解病毒的结构。计算机病毒在结构上有着共同性，一般由引导模块、传染模块、表现模块 3 部分组成。

注意：必须指出的是，不是任何病毒都必须包含这 3 个模块。

（1）引导模块。也就是病毒的初始化部分，它随着宿主程序的执行而进入内存，为传染模块做准备。

（2）传染模块。传染模块的作用是将病毒代码复制到目标上去。一般病毒在对目标进行传染前，要首先判断传染条件是否满足，判断病毒是否已经感染过该目标等。例如，CIH 病毒只针对 Windows 95/98 操作系统。

（3）表现模块。这是病毒间差异最大的部分，前两部分都是为这一部分服务的。它会破坏被传染系统或者在被传染系统的设备上表现出特定的现象。大部分病毒都是在一定条件下，才会触发其表现部分的。

2. 计算机病毒的工作机理

计算机病毒是可执行的程序，所以需要操作系统的支持。因为计算机病毒的传染和发作需要使用一些系统函数及硬件，而后者往往在不同的平台上是各不相同的，因此大多数计算机病毒都是针对某种处理器和操作系统编写的。

计算机病毒能够感染的只有可执行代码，按照可执行代码的种类可以将计算机病毒分为引导型病毒、文件型病毒、宏病毒和网络病毒四大类。

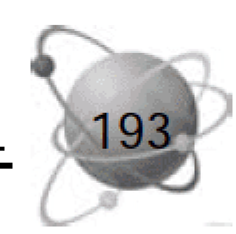
（1）引导型病毒

① 引导型病毒的工作机理

引导扇区是硬盘或软盘的第一个扇区，是存放引导指令的地方，这些引导指令对于操作系统的装载起着十分重要的作用。一般来说，引导扇区在 CPU 的运行过程中最先获得对 CPU 的控制权，病毒一旦控制了引导扇区，也就意味着病毒立即控制了整个计算机系统。

引导型病毒程序会用自己的代码替换原始的引导扇区信息，并把这些信息转移到磁盘的其他扇区中。当系统需要访问这些引导数据信息时，病毒程序会将系统引导到存储这些引导信息的新扇区，从而使系统无法发觉引导信息的转移，增强了病毒自身的隐蔽性。

引导型病毒可以将感染进行有效的传播。病毒程序将其部分代码驻留在内存中，这样



任何插入此系统驱动器中的磁盘都将感染此病毒。当这些感染了引导型病毒的磁盘在其他计算机系统中使用时，这个循环就可以继续下去了。

② 一个引导型病毒的例子

“巴基斯坦大脑”（Pakistani Brand）曾经是一种最流行的引导型病毒。它首先将原始的引导信息移动到磁盘的其他部分，然后将自己复制到引导扇区和磁盘的其他空闲区域，从而破坏了硬盘分区信息和文件定位表信息，导致用户无法访问文件。

“巴基斯坦大脑”病毒和其他的引导型病毒，都知道应该如何保护自己。该病毒能够在感染引导扇区之后仍旧若无其事地显示原始的、正确的引导扇区数据，而不是它自己的病毒代码。如果用户要删除或修改代码，该病毒能够自我毁灭，消除它自己的所有痕迹。令人感到奇怪的是，一方面“巴基斯坦大脑”病毒有许多逃避检测的功能，另一方面它又经常使用“（C）BRAIN”作为其卷标以显示它的存在。

（2）文件型病毒

① 文件型病毒的工作机理

文件型病毒攻击的对象是可执行程序，病毒程序将自己附着或追加在后缀名为.exe或.com 的可执行文件上。当感染了该类病毒的可执行文件运行时，病毒程序将在系统中进行它的破坏行动。同时，它将驻留在内存中，试图感染其他文件。当该类病毒完成了它的工作之后，其宿主程序才得到运行，使一切看起来很正常。

② 一个文件型病毒的例子

Lehigh 病毒是一种曾经广泛传播的文件型病毒。它将自己附加在一个 DOS 系统中非常重要的系统文件 COMMAND.COM 上，并通过软盘在计算机系统中传播。当某个计算机系统被该病毒感染了 4 次之后，它便开始删除硬盘上的信息，以致硬盘不可再用。

（3）宏病毒

随着 Microsoft 的办公自动化软件 Office 的日益普及，一种新型病毒——宏病毒开始流行开来。它在一定的条件下爆发，例如每月的 13 号，并且可以感染 Word 中的模板软件。

① 宏病毒的工作机理

为了减少用户的重复劳作，例如进行相似的操作，Office 提供了一种所谓宏的功能。利用这个功能，用户可以把一系列的操作记录下来，作为一个宏。之后只要运行这个宏，计算机就能自动地重复执行那些定义在宏中的所有操作。这种宏操作一方面方便了普通的计算机用户，另一方面却也给病毒制造者提供了可乘之机。

提示：简单地说，宏是一组批处理命令，是用高级语言编写的一段程序。

宏病毒是一种专门感染 Office 系列文档的恶性病毒。1995 年，世界上发现了第一个宏病毒 Concept。由于宏的编程语言 VBA 简单易学，因此大量的宏病毒层出不穷，短短两年时间其数量就上升至 20000 多种!

当 Word 打开一个扩展名为.doc 的文件时，首先检查里面有没有模板/宏代码。如果有，则认为这不是普通的.doc 文件，而是一个模板文件。如果里面存在以 AUTO 开头的宏，则 Word 随后就会执行这些宏。

染毒的.doc文件打开后，在用户使用菜单、快捷键和工具栏时，或者运行以AUTO开头的宏时，便会激活宏病毒，感染全局模板文件（例如，NORMAL.doc或POWERUP.doc等）。宏病毒通过控制这些全局模板文件，得到了系统的控制权。以后，当系统中有文档存储操作时，病毒就会将自身复制并入侵此文档文件，同时将该文档存储为一个扩展名为.doc的模板文件。当发作条件满足时，该病毒就会开始它的破坏活动。

除了Word宏病毒外，还出现了感染Excel、Access的宏病毒。宏病毒还可以在它们之间进行交叉感染，并由Word感染Windows的VxD。很多宏病毒具有隐形、变形能力，并具有对抗防病毒软件的能力。此外，宏病毒还可以通过电子邮件等进行传播。一些宏病毒已经不再在File Save As时暴露自己，并克服了语言版本的限制，可以隐藏在RTF格式的文档中。

② 一个宏病毒的例子

“台湾I号”和“台湾II号”就是两种宏病毒。它们在用户打开染毒的Word文档时，会给出一道数学题。如果用户答错了，它将打开10个文档窗口。然后，它又给出一道题，如果用户又算错了，它又会打开10个文档窗口……一直这样下去，直到消耗完该计算机上的系统资源，导致死机为止。

（4）网络病毒

为了更加容易理解，下面将以典型的“远程探险者”（Remote Explorer）病毒为例进行分析。为什么说它是典型的呢?因为它是真正的网络病毒，一方面它需要通过网络方可实施有效的传播；另一方面，它要想真正地攻入网络（无论是局域网还是广域网），本身必须具备系统管理员的权限，如果不具备此权限，则它只能够对当前被感染的主机中的文件和目录起作用。

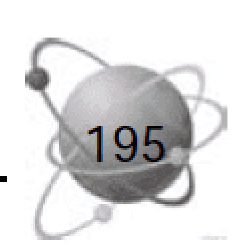
该病毒仅在Windows NT Server和Windows NT Workstation平台上起作用，专门感染.exe文件。Remote Explorer的破坏作用主要表现在：加密某些类型的文件，使其不能再用，并且能够通过局域网或广域网进行传播。

当具有系统管理员权限的用户运行了被感染的文件后，该病毒将会作为一项NT的系统服务被自动加载到当前的系统中。为增强自身的隐蔽性，该系统服务会自动修改Remote Explorer在NT服务中的优先级，在工作日（周一到周五）的6时到15时，Remote Explorer将自己的优先级设置为最低，而在其他时间则将自己的优先级提升一级，以便加快传染。

Remote Explorer的传播无须普通用户的介入（例如交换软盘或电子邮件等）。该病毒侵入网络后，直接使用远程管理技术监视网络，查看域登录情况并自动搜集远程计算机中的数据（包括超级用户口令），然后再利用所搜集的数据（例如口令）将自身向网络中的其他计算机传播。由于系统管理员能够访问到所有远程共享资源，所以具备同等权限的Remote Explorer也就能够感染网络环境中所有的NT服务器和工作站中的共享文件。

7.1.7 常见计算机网络病毒举例

据统计，目前世界上流行的计算机病毒达5万多种，而且几乎每月、每周都有新的病



毒及其变种产生。了解已知、常见和破坏力较强的病毒的特征，对病毒的诊断、清除和预防都是十分必要的。

下面将介绍 3 种较有代表性的计算机病毒：Internet 病毒、震荡波病毒和电子邮件病毒。

1. Internet 病毒

Internet 病毒是指美国一位 23 岁的学生莫里斯编制的计算机蠕虫（Worm）病毒。该病毒在 1988 年 11 月 2 日入侵了美国 Internet 网，殃及 5 个计算机中心的 12 个地区节点，连接着政府、大学、研究所和拥有政府合同的 25 000 多台计算机。据统计，这次病毒侵害造成的直接经济损失高达 9 600 万美元，而对各大研究中心和网络研究工作的影响更是难以估算。

这种病毒以三种途径侵入 Internet 网络：

（1）通过网络中 Berkeley UNIX 4.3 sendmail 的程序故障使调试位呈通态。

（2）在 finger 程序的一部分中使缓冲器过载，让其对病毒的另一部分进行编译和连接。

（3）通过获取口令进入系统。

病毒入侵后，通过网络不断扩散，使得受感染的系统负载变得非常重，直接影响网上 SUN 和 VAX 系统的运行。

2. “震荡波”病毒

2004 年 5 月 1 日，当人们正沉浸在黄金周的快乐之中时，一个新的病毒——“震荡波（Worm.Sasser）”开始在互联网上肆虐。

“震荡波”病毒跟“冲击波”病毒非常类似，它是利用微软的系统漏洞 MS04-011 进行传播的。用户的计算机一旦感染该病毒，系统将开启上百个线程去攻击他人，造成计算机系统运行异常缓慢、网络不畅通，并让系统不停地进行重新启动。

值得注意的是，在 2004 年 4 月 13 日，微软对此漏洞发布过级别为严重的安全公告。

据估计，该病毒的第一次爆发在中国造成了 10 万～20 万用户感染，仅在北京地区 5 天之内就殃及 7 000 用户，而从 5 月 8 日开始的第二次病毒爆发，给用户造成的损失更是远远超过第一次爆发。

如果计算机出现下列现象之一，则表明该计算机系统可能已经中毒，用户应该立刻采取措施，清除该病毒。

（1）出现系统错误对话框

首先，计算机出现如图 7-1 所示的 LSA Shell（Export Version）服务异常对话框，接着出现如图 7-2 所示的一分钟后重启计算机的“系统关机”提示对话框。

（2）系统资源被大量占用

病毒如果攻击成功，即会占用大量系统资源，使 CPU 占用率迅速达到 100%，出现计算机系统的运行异常缓慢、网络服务软件无法工作、速度突然变慢或断线、单击网页链接无响应、桌面或系统图标双击无法打开等现象。



图 7-1　LSA Shell（Export Version）服务异常对话框



图 7-2　“系统关机”对话框

（3）系统内存中出现名为 avserve 的进程

病毒如果攻击成功，会在内存中产生 avserve.exe 进程。可以通过按 Ctrl+Alt+Del 键的方式调用任务管理器，然后在“进程”选项卡中查看内存中是否存在该病毒进程。

（4）系统目录中出现名为 avserve.exe 的病毒文件

病毒如果攻击成功，会在系统安装目录（默认为 C:\WINNT）下生成一个名为 avserve.exe 的病毒文件。

（5）注册表中出现病毒键值

病毒如果攻击成功，会在注册表的 KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run 项中建立病毒键值"avserve.exe"="%WINDOWS%\ avserve.exe"。

3. 电子邮件病毒

臭名昭著的“美丽莎”（Melissa）、Papa 和 HAPPY99 以及“红色代码”等病毒，都是通过电子邮件的方式进行传播、扩散的，导致用户重要的文档泄密，甚至邮件服务器瘫痪，无法收发 E-mail，给个人、企业和政府部门造成了严重的损失。

所谓电子邮件病毒，就是以电子邮件方式作为传播途径的计算机病毒。

该类病毒的特点如下：

（1）电子邮件可以夹带任何类型的文件，夹带的文件可能带毒。

（2）有些计算机病毒，能自动通过电子邮件进行传染、扩散。

病毒通过电子邮件传播，具有以下两个特点：

（1）速度快，范围广。绝大多数通过电子邮件传播的病毒都具有自我复制的能力，它们能够主动选择用户邮箱地址簿中的地址自动发送邮件，或在用户发送邮件时，将被病毒感染的文件附到邮件上一起发送。这种成倍数增长的传播速度，可以使病毒在很短的时间内遍布整个 Internet 领域。

（2）破坏力大。通过电子邮件传播的病毒，其攻击的对象是整个计算机网络，因而其影响要远比单机染毒更大，破坏性也更强。

7.2　恶 意 代 码

恶意代码是一种程序，它通常在不被察觉的情况下把代码寄宿到另一段程序中，从而

达到破坏被感染的计算机数据、运行具有入侵性或破坏性的程序、破坏被感染的系统数据的安全性和完整性的目的。

7.2.1 常见的恶意代码

恶意代码的分类情况如图 7-3 所示。这些威胁可以分成两类：需要宿主的程序和可以独立运行的程序。前者实际上是程序片段，它们不能脱离某些特定的应用程序、应用工具或系统程序而独立存在；后者是完整的程序，操作系统可以调用和运行它们。

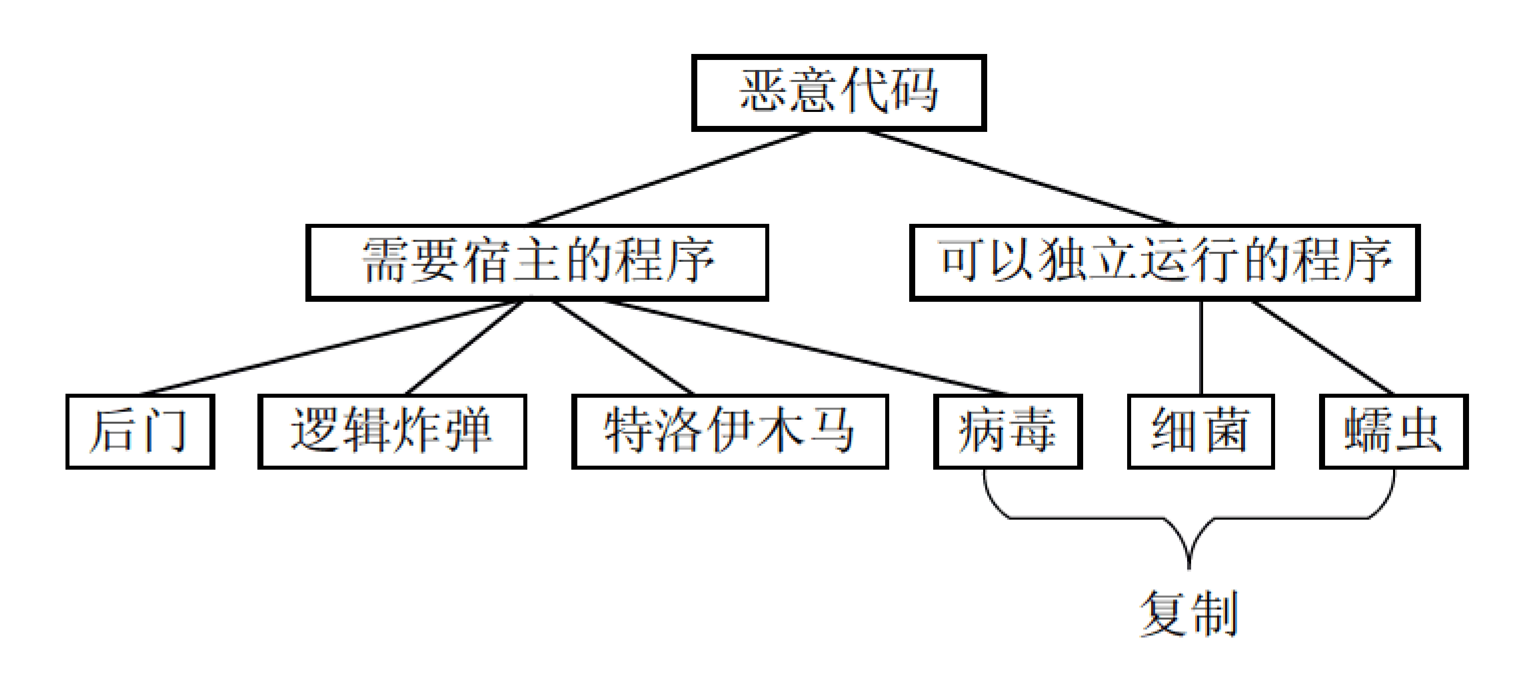


图 7-3 恶意代码分类示意图

也可以把这些软件威胁按照能不能够自我复制来进行分类。不能够自我复制的可能是程序片段，当调用宿主程序完成特定功能时，就会激活它们。可以自我复制的程序可能是程序片段（病毒），也可能是一个独立的程序（蠕虫、细菌）。当执行它们时，将会复制出一个或多个自身的副本，之后这些副本可以在同一个系统中或其他系统中被激活。

值得注意的是，随着恶意代码编写技术的提升，各种代码之间都在取长补短，所以有些恶意代码可能包含其他恶意代码。例如，“逻辑炸弹”或“特洛伊木马”可能是病毒或蠕虫的一部分。

1. 后门（Backdoor）

后门又称为陷阱门（Trapdoor），是进入程序的一个秘密入口，可以通过它绕过访问控制的一般安全检查，直接获得访问权限。很多年来，程序员为了调试和测试程序一直合法地使用后门；而当这些后门被用来获取非授权访问的权限时，它就变成了一种安全威胁。

2. 逻辑炸弹（Logic Bomb）

“逻辑炸弹”潜藏在合法程序中，当符合某种条件时就会“爆炸”。用来触发逻辑炸弹的条件可以是某些文件的出现或缺失、某个日期、某一特定用户运行该应用程序等。

3. 特洛伊木马（Trojan Horse）

“特洛伊木马”程序是一个表面看起来很有用的程序或命令过程，其中包含了秘密代码。当调用的时候，这些秘密代码将执行一些不必要的或有害的操作。

当未授权用户无法直接完成某些操作的时候，就可以通过“特洛伊木马”程序来间接

完成。例如，在一个多用户操作系统中，如果想访问其他用户的文件，那么恶意用户就可以创建一个“特洛伊木马”程序，当执行它的时候，将改变用户文件的访问权限。攻击者为了诱使用户运行该程序，会把它放在公共目录里，并给它取一个听起来好象是一个很有用的程序的名字。当另一个用户运行该程序后，攻击者就能够访问该用户的文件信息了。

很难被检测到的一种“特洛伊木马”程序就是编译器。通过修改正常的编译器，就可以在编译某些程序的时候插入附加代码，如在登录程序中留下后门，这样攻击者就可以使用特殊的口令登录到系统中。

4．病毒（Virus）

病毒是指能够通过修改其他程序而“感染”它们的一种程序。修改以后的程序里面包含了病毒程序的一个副本，这样它们就能够继续感染其他程序。

5．蠕虫（Worm）

网络蠕虫通过网络连接，利用多种方法从一个系统向另一个系统传播。一旦在一个系统中激活，网络蠕虫就能够像计算机病毒或细菌一样活动。它也能植入“特洛伊木马”程序或执行一些破坏性动作。

7.2.2 木马

1．木马病毒概述

“特洛伊木马”的英文名称为 Trojan Horse（其名称取自希腊神话的《特洛伊木马记》），是指表面看上去对人们有用或有趣，但实际上却有害的东西，并且它的破坏性是隐蔽的。

计算机中的木马是一种基于远程控制的黑客工具，采用客户机/服务器工作模式。它通常包含控制端和被控制端两部分。被控制端的木马程序一旦植入受害者的计算机（简称宿主）中，操纵者就可以在控制端实时监视该用户的一切操作，有的放矢地窃取重要文件和信息，甚至还能远程操控受害计算机对其他计算机发动攻击。木马的控制端和被控制端通过网络进行交互。

“特洛伊木马”是一种恶意程序，它们悄悄地在寄宿主机上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。一般而言，大多数“特洛伊木马”都会模仿一些正规的远程控制软件（例如 Symantec 的 pcAnywhere）的功能，但其独特之处还是很明显的，例如它的安装和操作都在隐蔽之中完成。攻击者经常把“特洛伊木马”隐藏在一些游戏或小软件之中，诱使粗心的用户在自己的机器上运行。最常见的情况是，上当的用户有的是从不正规的网站下载和运行了带恶意代码的软件，有的是不小心单击了带恶意代码的邮件附件。

木马的运行，可以采用以下 3 种模式。

（1）潜伏在正常的程序应用中，附带执行独立的恶意操作。

（2）潜伏在正常的程序应用中，但会修改正常的应用进行恶意操作。

（3）完全覆盖正常的程序应用，执行恶意操作。

2．木马的特点

木马具有隐蔽性和非授权性的特点。

所谓隐蔽性，是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马。这样，被控制端即使发现感染了木马，也不能确定其准确的位置。

所谓非授权性，是指一旦控制端与被控制端连接后，控制端将享有被控制端的大部分操作权限，包括修改文件、修改注册表、控制鼠标、键盘等，这些权力并不是被控制端赋予的，而是通过木马程序窃取的。

3．木马的工作过程

木马对网络主机的入侵过程，可大致分为 6 个步骤。

（1）配置木马

一般来说，一个设计成熟的木马都有木马配置程序。

从具体的配置和内容来看，主要是为了实现木马伪装和信息反馈两个功能。

木马配置程序为了在被控制端尽可能地隐藏好木马，会采用多种伪装手段，例如修改图标、捆绑文件、定制端口、自我销毁等。

木马配置程序将就信息反馈的方式或地址进行设置，例如设置信息反馈的邮件地址、IRC 号或 ICQ 号等。

（2）传播木马

木马的传播方式主要有 3 种：一种是通过 E-mail，控制端将木马程序以附件形式附着在邮件上发送出去，收件人只要打开附件就会感染木马；第二种是软件下载，一些非正规的网站以提供软件下载的名义，将木马捆绑在软件安装程序上，程序下载后只要一运行这些程序，木马就会自动安装；第三种是通过即时通信软件（例如 QICQ）的“传送文件”进行传播，不知情的网友一旦打开带有木马的文件就会感染木马。

（3）运行木马

被控制端用户运行感染或捆绑木马的程序后，木马就会自动进行安装。它首先会将自身复制到 Windows 的系统文件夹中，然后在注册表、启动组、非启动组中设置好触发条件，完成安装。

当木马运行的触发条件满足时，木马便被激活，然后进入内存，并开启事先定义好的木马端口，准备与控制端建立连接。

（4）信息泄露

一般来说，设计成熟的木马都有一个信息反馈机制。

所谓信息反馈机制，是指木马成功安装后，会收集一些被控制端的软、硬件信息，并通过 E-mail、IRC 或 ICQ 的方式告知控制端用户。

（5）连接建立

一个木马连接的建立，首先必须满足两个条件：一是被控制端已安装了木马程序；二是控制端、被控制端都要在线。在此基础上，控制端可以通过木马端口，与被控制端建立

连接。

（6）远程控制

木马连接建立后，控制端端口和木马端口之间将会出现一条通道，控制端上的控制端程序可借助于这条通道，与被控制端上的木马程序取得联系，并通过木马程序对被控制端进行远程控制。

控制操作包括：窃取密码、文件操作、修改注册表和系统操作等。

4. 木马的危害

木马是一种远程控制工具，以简便、易行、有效而深受黑客青睐。木马主要以网络为依托进行传播，窃取用户隐私资料是其主要目的；而且多具有引诱性与欺骗性，是病毒新的危害趋势。

木马可以说是一种后门程序，它会在受害者的计算机系统里打开一个“后门”，黑客经由这个被打开的特定“后门”进入系统，然后就可以随心所欲地操纵计算机了。那么黑客通过木马进入到计算机里后能够做什么呢?有的木马具有捕获每一个用户屏幕、每一次击键事件的能力；有的木马能够随意操控宿主主机的资源，例如 2004 年 6 月发现的“蜜蜂大盗”可以打开主机上连接的摄像头、麦克风，并将得到的图像、声音传给木马控制者；有的木马能够冒充宿主主机的合法用户进行诸如发送邮件、修改文档，甚至银行转账等操作；有的木马能够捕获和分析流经网卡的每一个数据包等。感染了木马的系统，用户的一切秘密都将暴露在别人面前，隐私将不复存在。

“特洛伊木马”控制者既可以随心所欲地查看被入侵的机器，也可以用广播方式发布命令，指示所有在其控制下的“特洛伊木马”一起行动，或者向更广泛的范围传播，或者做其他危险的事情。实际上，只要用一个预先定义好的关键词，就可以让所有被入侵的机器格式化自己的硬盘，或者向另一台主机发起攻击。攻击者经常会用“特洛伊木马”侵占大量的机器，然后针对某一要害主机发起分布式拒绝服务攻击（DDoS）。

木马在黑客入侵中也是一种不可缺少的工具。美国微软公司曾于 2000 年 10 月 27 日宣布一名黑客入侵了其门户网站，而网站的一些内部信息则是被一种叫做 QAZ 的木马传出去的。

木马不仅是一般黑客的常用工具，更是网上情报刺探的一种主要手段，对国家安全造成了巨大威胁。

我国国家计算机网络安全应急技术处理协调中心发布的 2007 年上半年网络安全报告中，特别提到了对国家安全造成严重危害的两种网络安全威胁，其中之一就是木马。报告指出，2007 年上半年我国大陆地区大量主机被境外植入木马程序，这些被植入了木马被控制端的主机主要分布在上海、北京和江苏；同时在大陆地区外的木马控制端有数万个，其中位于我国台湾地区的最多，占总数的 42%，位于美国的也占了约 25%。

在一起网络间谍案的调查过程中，我国有关部门从政府某部门及其对口地方单位的计算机网络中检测出了不少特制的木马程序，所有入侵木马的连接都指向境外的特定间谍机构。专业部门进行检测时，测出的木马很多还正在下载、外传资料，专业人员当即采取措

施，制止了进一步的危害。

有时网上间谍还会运用社会工程学，结合电子邮件欺骗植入木马。曾经有一个真实的案例，一家涉密单位的工作人员收到了“上级机关”发来的一封电子邮件，内容是“病毒木马检测程序”。一看是自己人，来信又正好对路，工作人员没有多想就打开信件，运行程序，结果境外间谍机关的木马一下植入计算机中，原来所谓的“上级机关”是境外网络间谍假冒的。

很多保密单位的内部工作网是不与互联网连接的，但有关部门进行安全检测时仍然从中发现了许多境外情报部门的木马。调查表明，其中一个重要的途径便是摆渡攻击，即利用像 U 盘、移动硬盘之类的移动介质。境外间谍部门专门设计了各种各样的摆渡木马，并且搜集了我国大量保密单位工作人员的个人网址或邮箱。只要这些人当中有联网使用 U 盘等移动介质的，摆渡木马就会悄悄植入移动介质。一旦这些人违规在内部工作网的计算机上插入 U 盘等移动介质，摆渡木马立刻就会感染内网，把保密资料下载到移动介质上。完成这样的摆渡后，只要使用者再把这个移动介质接入联网计算机，下载的情报就会自动传到控制端的网络间谍那里。

2004 年国内危害最严重的 10 种木马是：QQ 木马、网银木马、MSN 木马、传奇木马、剑网木马、BOT 系列木马、灰鸽子、蜜蜂大盗、黑洞木马、广告木马。这些木马会随着电子邮件、即时通信工具、网页浏览等方式感染用户计算机。系统漏洞就像给了木马一把钥匙，使它能够很轻易地在计算机中潜伏下来，达到其窃取隐私信息的险恶目的。

根据木马的特点及其危害范围，可将其分为针对网络游戏的木马、针对网上银行的木马、针对即时通信工具的木马、给计算机开后门的木马和推广广告的木马五大类别。

（1）网游木马。2004 年，针对网络游戏的木马不断涌现。究其原因，主要是网络游戏产业超高速发展，网上虚拟装备交易非常火爆而安全性却比较薄弱。这就给了一些别有用心的病毒作者兴风作浪的机会。如果中了针对网络游戏的木马，用户账号就会被盗取，并立即将账号中的游戏装备转移，再由木马病毒使用者卖出这些被盗取的游戏装备而获利。如今，有些人干脆以制作木马为职业。

（2）网银木马。网银木马专门针对网上银行发起攻击，采用记录键盘和系统动作的方法盗取他人网银的账号和密码，并发送到作者指定的邮箱，直接导致用户的经济损失。目前通过网络银行的犯罪行为已经开始出现，某大学生利用网络偷取网络银行用户 60 多万元人民币，还试图用钱贿赂办案警察，但最终还是受到了法律的严惩。

（3）即时通信木马。该类木马可以利用即时通信工具（例如 QQ、MSN）进行传播。中了木马后计算机会下载病毒和作者指定的任意程序，其危害不可确定。有时也可能会造成恶作剧，例如“MSN 我要结婚”病毒，中毒者会向联系人发送“我今天要结婚”的恶作剧消息。

（4）后门木马。该类木马在网络中被恶意者大量传播。该类木马采用反弹端口技术绕过防火墙，对被感染的系统进行远程文件和注册表的操作，可以捕获被控制的计算机屏幕、重启和关闭计算机、禁用系统热键和注册表编辑器。中了该类木马后，被感染的系统将完全控制在黑客手中。

（5）广告木马。此类木马采用各种技术隐藏于系统内，修改 IE 等网页浏览器的主页，禁止多种系统功能，收集系统信息发送给传播广告木马的网站。更恶毒的是修改网页定向，导致一些正常的网站不能登录。MSN 病毒就是这种木马，它诱使用户单击一个可执行文件，就导致了 900 多个网站不能正常访问。

这五大类木马基本构成了木马的主体，其中网游木马占木马病毒总数的 32%以上，网银木马占 7%，即时通信木马占 23%，广告木马占 24%，后门木马占 14%。从危害程度来看，网游木马危害最为严重，其次是广告木马、即时通信木马、后门木马，最后是网银木马。

5. 木马的检测和清除

可以通过查看系统端口开放的情况、系统服务情况、系统任务运行情况、网卡的工作情况、系统日志及运行速度有无异常等对木马进行检测，检测到计算机感染木马后，就要根据木马的特征来进行清除；此外，也可查看是否有可疑的启动程序、可疑的进程存在，是否修改了 Win.ini、System.ini 系统配置文件和注册表，如果存在可疑的程序和进程，则按照特定的方法进行清除。

（1）查看开放端口

当前最为常见的木马通常是基于 TCP/UDP 协议进行客户端与服务器端之间通信的，因此我们可以通过查看在本机上开放的端口，看是否有可疑的程序打开了某个可疑的端口。例如，“冰河”木马使用的监听端口是 7626，Back Orifice 2000 使用的监听端口是 54320 等。假如查看到有可疑的程序在利用可疑端口进行连接，则很有可能就是感染了木马。查看端口的方法通常有以下几种：

- 使用 Windows 本身自带的 netstat 命令。
- 使用 Windows 下的命令行工具 fport。
- 使用图形化界面工具 Active Ports。

（2）查看和恢复 Win.ini 和 System.ini 系统配置文件

查看 Win.ini 和 System.ini 文件是否有被修改的地方。例如，有的木马通过修改 Win.ini 文件中 Windows 节下的“load=file.exe，run=file.exe”语句进行自动加载，还可能修改 System.ini 中的 boot 节，实现木马加载。例如，“妖之吻”病毒将 Windows 系统的图形界面命令解释器“shell=explorer.exe”修改成“shell=yzw.exe”，在计算机每次启动后就自动运行程序 yzw.exe。此时可以把 System.ini 恢复为原始配置，即将“shell=yzw.exe”修改回“shell=explorer.exe”，再删除掉病毒文件即可。

（3）查看启动程序并删除可疑的启动程序

如果木马自动加载的文件是直接通过在 Windows 菜单中自定义添加的，一般都会放在主菜单的“开始”→“程序”→“启动”处，在 Windows 资源管理器里的位置是“C:\Windows\startmenu\programs\启动”处。通过这种方式使文件自动加载时，一般都会将其存放在注册表中下述 4 个位置上：

- HKEY_CURRENT_user\software\microsoft\windows\currentversion\explorer\shellfolders
- HKEY_CURRENT_user\software\microsoft\windows\currentversion\explorer\userShellfolders

- HKEY_LOCAL_machine\software\microsoft\windows\currentversion\explorer\userShellFolders
- HKEY_LOCAL_machine\software\microsoft\windows\eurrentversion\explorer\shellfolders

检查是否有可疑的启动程序，便很容易查到是否感染了木马。如果查出有木马存在，则除了要查出木马文件并删除外，还要将木马自动启动程序删除。

（4）查看系统进程并停止可疑的系统进程

木马再狡猾，也只是一个应用程序，需要进程来执行。可以通过查看系统进程来推断木马是否存在。在 Windows NT/XP 系统下，按 Ctrl+Alt+Del 键进入任务管理器，就可看到系统正在运行的全部进程。在 Windows 下，可以通过 proview 和 winproc 工具来查看进程。在查看进程时，如果对系统非常熟悉，对系统运行的每个进程知道它是做什么的，那么在木马运行时，就能很容易发现哪个是木马程序的活动进程了。

在对木马进行清除时，首先要停止木马程序的系统进程。例如，Hack.Rbot 病毒除了将自身复制到一些固定的 Windows 自启动项中外，还在进程中运行 wuamgrd.exe 程序，修改注册表，以便病毒可随时自启动。看到有木马程序在运行时，需要马上停止系统进程，并进行下一步操作，修改注册表和清除木马文件。

（5）查看和还原注册表

木马一旦被加载，一般都会对注册表进行修改。通常木马在注册表中实现加载文件是在以下几处：

- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run
- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runonce
- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runservices
- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runservicesonce
- HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\runonce
- HKEY_CURRENT_USER\software\microsoft\windows\currentversion\runservices

此外，在注册表中的 HKEY_CLASSES_ROOT\exefile\shell\open\command=“%1” %*处，如果其中的“%1”被修改为木马，那么每启动一次该可执行文件木马就会启动一次。

查看注册表，将注册表中木马修改的部分还原。例如，Hack.Rbot 病毒已向注册表的有关目录中添加键值“MicrosoftUpdate=wuamgrd.exe”，以便病毒可随机自启动。这就需要先进入注册表，将键值“MicrosoftUpdate=wuamgrd.exe”删除掉。值得注意的是，可能有些木马会不允许执行.exe 文件，这时就要先将 regedit.exe 改成系统能够运行的形式，如改成 regedit.com。

（6）使用杀毒软件和木马查杀工具检测和清除木马

最简单的检测和删除木马的方法是安装木马查杀软件，例如 KV 3000、瑞星、TheCleaner、“木马克星”、“木马终结者”等。此外，McAfee Virus Scan 和 Anti-TrojanShield 也是不错的木马查杀工具。McAfee Virus Scan 集合了入侵防卫及防火墙技术，为个人计算机和文件服务器提供全面的病毒防护；Anti-TrojanShield 是一款享誉欧洲的专业木马检测、拦截及清除软件。

多数情况下由于杀毒软件和查杀工具的升级慢于木马的出现，因此学会手工查杀也是非常必要的。手工查杀木马的方法如下：

（1）检查注册表

查看 HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion 和 HKEY_CURRENT_USER\software\microsoft\windows\currentversion 下所有以 run 开头的键值名下有没有可疑的文件名。如果有，就需要删除相应的键值，再删除相应的应用程序。

（2）检查启动组

虽然启动组不是十分隐蔽，但这里的确是自动加载运行的好场所，因此可能有木马隐藏其中。启动组对应的文件夹为 C:\windows\startmenu\programs\startup，要注意经常对其进行检查，发现木马后及时清除。

（3）查看 Win.ini 和 System.ini

Win.ini 以及 System.ini 也是木马喜欢的隐蔽场所，要注意这些地方。例如，Win.ini 的 Windows 小节下的 load 和 run 后面在正常情况下是没有跟什么程序的，在这里如果发现有程序就要小心了，它很有可能便是木马被控制端程序，应尽快对其进行检查并清除。

（4）查看 C:\WINDOWS\winstart.bat 和 C:\WINDOWS\wininit.ini

对于文件 C:\WINDOWS\winstart.bat 和 C:\WINDOWS\wininit.ini 也要多加检查，木马也很可能隐藏在这里。

（5）查看可执行文件

如果是由.exe 文件启动，那么运行这个程序，看看木马是否被装入内存，端口是否打开。如果是，则说明要么是该文件启动了木马程序，要么是该文件捆绑了木马程序。最好将其删除，再重新安装一个这样的程序。

6. 木马的预防

目前木马已对计算机用户信息安全构成了极大威胁，做好木马的防范工作刻不容缓，用户必须提高警惕，尤其是网络游戏玩家更应该提高对木马的关注。

网络中流行的木马程序通常传播速度比较快，影响比较严重，因此尽管可以利用一些工具方法来检测、清除木马，但只能是亡羊补牢，比较被动。当然最好的情况是不出现木马，这就要求我们平时要有对木马的预防意识和措施，做到防患于未然。以下是几种简单适用的木马预防方法和措施：

（1）不随意打开来历不明的电子邮件，阻塞可疑邮件

现在许多木马都是通过电子邮件来传播的，当收到来历不明的邮件时，不要轻易打开；并加强邮件监控系统，拒收垃圾邮件。可通过设置邮件服务器和客户端来阻塞带有可疑附件的邮件，例如附件的扩展名与恶意代码有关联（例如.pif、.vbs），或是带有复合扩展名的可疑邮件（例如.txt.vbs、.htm.exe 等）。

（2）不随意下载来历不明的软件

最好是在一些知名的网站下载软件，不要下载和运行那些来历不明的软件。在安装软件之前，最好用杀毒软件查看有没有病毒，然后再安装。

（3）及时修补漏洞和关闭可疑的端口

一般木马都是通过漏洞在系统上打开端口留下后门的，在修补漏洞的同时要对端口进

行检查，把可疑的端口关闭。

（4）尽量少用共享文件夹

尽量少用共享文件夹，如果必须使用，则应设置账号和密码保护。千万不要将系统目录设置成共享，最好将系统下默认共享的目录关闭。

注意：Windows 系统在默认情况下将目录设置成共享状态。

（5）运行实时监控程序

在上网时最好运行反木马实时监控程序和个人防火墙，并定时对系统进行病毒检测。

（6）经常升级系统和更新病毒库

经常关注厂商网站的安全公告，因为这些网站通常都会及时地将漏洞、木马和更新公布出来，并在第一时间发布补丁和新的病毒库等。

（7）限制使用不必要的具有传输能力的文件

限制使用诸如点对点传输软件、音乐共享软件、即时通信软件等，因为这些程序经常被用来传播恶意代码。

7.2.3　蠕虫

网络蠕虫作为对互联网危害严重的一种计算机程序，其破坏力和传染性不容忽视。与传统的病毒不同，蠕虫病毒以计算机为载体，以网络为攻击对象。

1. 蠕虫的定义

计算机病毒自出现之日起，就成为计算机系统的一个巨大威胁，而当网络迅速发展的时候，蠕虫病毒引起的危害开始显现。

蠕虫病毒和普通病毒有着很大的区别。普通病毒是需要寄生的，它可以通过自身指令的执行，将自己的指令代码寄宿到其他程序体内，而被感染的文件就被称为“宿主”。宿主程序执行的时候，就可先执行病毒程序，病毒程序运行完之后，再把控制权交给宿主原来的程序指令。由此可见，普通病毒主要是感染文件和引导区，而蠕虫则是一种通过网络进行传播的恶性代码。它具有普通病毒的一些共性，例如传播性、隐蔽性、破坏性等；同时也具有一些自己的特征，例如不利用文件寄生、可对网络造成拒绝服务、与黑客技术相结合等。蠕虫的传染目标是网络内的所有计算机。在破坏性上，蠕虫病毒也不是普通病毒所能比的，网络的发展使得蠕虫可以在短短的时间内蔓延到整个网络，造成网络瘫痪。蠕虫病毒与一般病毒的区别如表 7-1 所示。

表 7-1　蠕虫病毒与一般病毒的区别

	普 通 病 毒	蠕 虫 病 毒
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

2. 蠕虫的分类

（1）根据使用者情况的不同，可将蠕虫病毒分为两类，即面向企业用户的蠕虫病毒和面向个人用户的蠕虫病毒。

面向企业用户的蠕虫病毒利用系统漏洞，主动进行攻击，可以对整个网络造成瘫痪性的后果，以“红色代码”、“尼姆达”、“SQL 蠕虫王”为代表；面向个人用户的蠕虫病毒通过网络（主要是电子邮件、恶意网页形式等）迅速传播，以“爱虫”、“求职信”蠕虫为代表。

在这两类蠕虫病毒中，第一类具有很大的主动攻击性，而且发作也有一定的突然性，但相对来说，查杀这种蠕虫并不很难；第二种蠕虫的传播方式比较复杂和多样，少部分利用了微软的应用程序漏洞，大部分是利用社会工程学（Social Engineering）陷阱对用户进行欺骗和诱使，这样的蠕虫造成的损失是非常大的，同时也是很难根除的。例如，“求职信”蠕虫在 2001 年就已经被各大杀毒厂商发现，但直到 2002 年底依然处于蠕虫危害排行榜的首位。

（2）按其传播和攻击特征，可将蠕虫病毒分为 3 类，即漏洞蠕虫、邮件蠕虫和传统蠕虫病毒。

其中以利用系统漏洞进行破坏的蠕虫病毒最多，占蠕虫病毒总数量的 69%；邮件蠕虫居第二位，占蠕虫病毒总数量的 27%；其他传统蠕虫病毒占 4%。

蠕虫病毒可以造成互联网大面积瘫痪，引起邮件服务器堵塞，最主要的症状表现在用户浏览不了互联网，或者企业用户接收不了邮件。例如，2004 年爆发的“震荡波”病毒造成了互联网大面积瘫痪，众多用户无法使用互联网；“五毒虫”蠕虫病毒可以堵塞企业邮件服务器，造成邮件病毒泛滥。

漏洞蠕虫可利用微软的系统漏洞进行传播，主要是 SQL 漏洞、RPC 漏洞和 LSASS 漏洞，其中 RPC 漏洞和 LSASS 漏洞最为严重。漏洞蠕虫极具危害性，大量的攻击数据堵塞网络，并可造成被攻击系统不断重启、系统速度变慢等故障。漏洞蠕虫的特性若被集成到黑客病毒，造成的危害就更大了。

邮件蠕虫主要通过电子邮件进行传播。邮件蠕虫使用自己的 SMTP 引擎，将病毒邮件发送给搜索到的邮件地址。邮件蠕虫还能利用 IE 漏洞，使用户在没有打开附件的情况下感染病毒。最新的 MYDOOM 变种 AH 甚至能利用 IE 漏洞，使病毒邮件不再需要附件就可感染用户。

3. 蠕虫的基本结构

蠕虫的基本程序结构包含传播模块、隐藏模块和目的功能模块。

（1）传播模块。该模块的功能是负责蠕虫的传播。传播模块又可以分为 3 个基本模块，即扫描模块、攻击模块和复制模块。

（2）隐藏模块。该模块的功能是病毒侵入主机后，隐藏蠕虫程序，防止被用户发现。

（3）目的功能模块。该模块的功能是实现对计算机的控制、监视或破坏等。

4. 蠕虫的传播

局域网条件下的共享文件夹、电子邮件和网络中的恶意网页、大量存在着漏洞的服务器等都成为蠕虫传播的途径。网络的发展也使得蠕虫病毒可以在几个小时内蔓延到全球，而且蠕虫的主动攻击性和突然爆发性将使得人们束手无策。

蠕虫程序的一般传播过程如下：

（1）扫描。由蠕虫的扫描功能模块负责收集目标主机的信息，寻找可利用的漏洞或弱点。当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象。扫描采用的技术方法包括用扫描器扫描主机，探测主机的操作系统类型、主机名、用户名、开放的端口、开放的服务、开放的服务器软件版本等。

（2）攻击。攻击模块按步骤自动攻击前面扫描中找到的对象，取得该主机的权限（一般为管理员权限），获得一个 Shell。

（3）复制。复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机中并启动。

5. 蠕虫的破坏性

1988 年，一个由美国某大学研究生莫里斯编写的蠕虫病毒首次现身网络并迅速蔓延，造成数千台计算机停机；而后来的“红色代码”、“尼姆达病毒”疯狂时，曾造成几十亿美元的损失；2003 年初，一种名为“SQL 蠕虫王”的病毒迅速传播并袭击了全球，致使互联网严重堵塞，作为互联网主要基础的域名服务器 DNS 受到侵袭，而网民浏览互联网网页及收发电子邮件的速度大幅降低，同时银行自动取款机运行中断，网络机票预订系统运行中断，信用卡收付款系统出现故障等。据专家估计，此次病毒造成的直接经济损失至少在 26 亿美元以上。由此可见，蠕虫病毒对网络具有严重的破坏性，并造成巨大的经济损失。

表 7-2 列出了一些有代表性的蠕虫的发作时间及其破坏性。

表 7-2　著名蠕虫病毒的发作时间和破坏性

病毒名称	发作时间	特点及造成损失
莫里斯蠕虫	1988 年	6000 多台计算机停机，直接经济损失高达 9600 万美元
美丽莎	1999 年	政府部门和一些大公司紧急关闭了网络服务器，经济损失超过 12 亿美元
爱虫病毒	2000 年 5 月	众多用户计算机被感染，损失超过 100 亿美元以上
红色代码	2001 年 8 月	网络瘫痪，直接经济损失超过 26 亿美元
尼姆达	2001 年 9 月	通过电子邮件、网络共享、IIS 漏洞和网络浏览等多途径传播，造成众多网络瘫痪
求职信	2001 年 10 月	大量病毒邮件堵塞服务器，损失达数百亿美元
SQL 蠕虫王	2003 年 1 月	网络大面积瘫痪，银行自动取款机运行中断，直接经济损失超过 26 亿美元
冲击波	2003 年 8 月	利用 RPC 漏洞传播，并相继出现了病毒变种和一系列利用 RPC 漏洞传播的病毒。数日内，国内数百万台计算机被攻击
震荡波	2004 年 5 月 1 日	三天内出现第二个变种，破坏性超过“冲击波”病毒，全球各地上百万用户遭到攻击，并造成重大损失

表 7-2 所列出的蠕虫病毒中，“爱虫”蠕虫病毒开创了在局域网内主动扫描传播的新方式；“红色代码”蠕虫病毒开创了利用微软系统漏洞传播病毒的先河；而“尼姆达”和“震荡波”蠕虫病毒则综合了以上两种方式，成为超级病毒。

6. 蠕虫的特点

通过对以上蠕虫病毒的分析，可见蠕虫病毒具有以下特点。

（1）传播迅速，难以清除。一旦某台计算机感染了蠕虫病毒，在短时间内，几乎网络上所有的计算机都会被依次传染，同时网络出现各种异常状况甚至发生阻塞，严重影响网络的正常使用；而且系统感染这些病毒后，很难清除。

（2）利用操作系统和应用程序的漏洞主动进行攻击。此类蠕虫主要是“红色代码”、“尼姆达”和“震荡波”等。由于 IE 浏览器的漏洞，使得感染了“尼姆达”蠕虫的邮件在不用手工打开附件的情况下病毒就能激活，而此前即便是很多防病毒专家也一直认为，只要不去打开带有病毒附件的邮件，病毒就不会有危害。“红色代码”利用微软 IIS 服务器软件的 idq.dll 远程缓存区溢出漏洞来传播，“震荡波”病毒利用微软操作系统漏洞 LSASS 进行攻击，“SQL 蠕虫王”病毒则是利用微软的数据库系统的一个漏洞进行大肆攻击。

（3）传播方式多样。一些蠕虫可利用的传播途径包括文件、电子邮件、Web 服务器、网络共享等。

（4）病毒制作技术与传统的病毒不同。许多新的蠕虫病毒是利用当前最新的编程语言与编程技术实现的，易于修改以产生新的变种，从而躲避防病毒软件的搜索。另外，新病毒利用 JavaScript、ActiveX、VB Script 等技术，可以潜伏在 HTML 页面中，在用户上网浏览时触发。

（5）与黑客技术相结合。蠕虫和黑客技术的结合，使得对蠕虫的分析、检测和防范具有一定的难度。以“红色代码”蠕虫病毒为例，被感染机器的 Web 目录\scripts 下将生成一个 root.exe，可以远程执行任何命令，从而使黑客能够再次进入，潜在的威胁和损失更大。

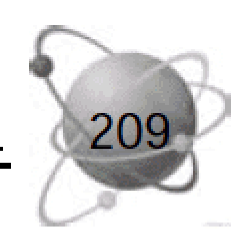
7. 蠕虫病毒的防范

与普通病毒不同，蠕虫病毒往往能够利用漏洞来入侵、传播。这里的漏洞（或者说是缺陷）分为软件缺陷和人为缺陷两类。软件缺陷（例如远程溢出、微软 IE 和 Outlook 的自动执行漏洞等）需要软件厂商和用户共同配合，不断地升级软件来解决。人为缺陷主要是指计算机用户的疏忽。当收到一封带有病毒的求职邮件时，大多数人都会去单击，这就是所谓的社会工程学。对于企业用户来说，威胁主要集中在服务器和大型应用软件上；而对个人用户，主要是防范第二种缺陷。

（1）企业类蠕虫病毒的防范

2002 年 7 月，微软的安全公告中就对“SQL 蠕虫”病毒利用的漏洞作了详细的说明，而且微软也提供了安全补丁程序，然而在病毒发作时还是有相当多的服务器没有安装最新的补丁，其网络管理员的安全防范意识可见一斑。

当前，企业网络主要应用于文件和打印服务共享、办公自动化系统、企业管理信息系统 MIS、Internet 应用等领域。网络具有便利的信息交换特性，蠕虫病毒也可以充分利用网



络快速传播以达到其阻塞网络的目的。企业在充分利用网络进行业务处理的同时，也要考虑病毒的防范问题，以保证关系企业命运的业务数据的完整性和可用性。

企业防治蠕虫病毒需要考虑病毒的查杀能力、病毒的监控能力和新病毒的反应能力等几个问题。而企业防病毒的一个重要方面就是管理策略，现建议企业防范蠕虫病毒的策略如下：

① 加强网络管理员的安全管理水平，提高安全意识。由于蠕虫病毒利用的是系统漏洞，所以需要在第一时间保持系统和应用软件的安全性，保持各种操作系统和应用软件的更新。由于各种漏洞的出现，使得安全问题不再是一劳永逸的事，而作为企业用户而言，所经受攻击的危险也是越来越大，要求企业的管理水平和安全意识也越来越高。

② 建立病毒检测系统，能够在第一时间内检测到网络的异常和病毒的攻击。

③ 建立应急响应系统，将风险降到最低。由于蠕虫病毒爆发的突然性，可能在病毒发现的时候已经蔓延到了整个网络，所以建立一个紧急响应系统是很有必要的，在病毒爆发的第一时间即能提供解决方案。

④ 建立备份和容灾系统，对于数据库和数据系统，必须采用定期备份、多机备份和容灾等措施，防止意外灾难下的数据丢失。

（2）个人用户蠕虫病毒的分析和防范

对于个人用户而言，威胁大的蠕虫病毒一般采取电子邮件和恶意网页传播方式。这些蠕虫病毒对个人用户的威胁最大，同时也最难以根除，造成的损失也更大。

对于利用电子邮件传播的蠕虫，通常利用的是社会工程学欺骗，即以各种各样的欺骗手段诱惑用户单击的方式进行传播。确切地说，恶意网页是一段黑客代码程序，它内嵌在网页中，当用户在不知情的情况下将其打开时，病毒就会发作。这种病毒代码内嵌技术的原理并不复杂，所以能够很容易地被利用。在很多黑客网站中竟然出现了关于用网页进行破坏的技术论坛，并提供破坏程序代码下载，从而造成了恶意网页的大面积泛滥，也使越来越多的用户遭受损失。

通过上述的分析可知，病毒并不是非常可怕的，网络蠕虫对个人用户的攻击主要还是通过社会工程学，而不是利用系统漏洞，所以防范此类病毒需要注意以下几点。

（1）购买合适的杀毒软件。

（2）经常升级病毒库。

（3）提高防杀病毒意识。

（4）不随意查看陌生邮件，尤其是带有附件的邮件。

7.3　计算机病毒的检测与清除

目前病毒的破坏力越来越强，几乎所有的软、硬件故障都可能与病毒有牵连。所以，当操作时发现计算机有异常情况，首先应怀疑的就是病毒在作怪，而最佳的解决办法就是利用杀毒软件对计算机进行一次全面的清查。

7.3.1 计算机病毒的传播途径

计算机病毒是通过某个入侵点进入系统进行传染的。最常见的入侵点是从工作站传到工作站的软盘或 U 盘等移动存储设备。在网络中可能的入侵点还有服务器、E-mail、BBS 上下载的文件、WWW 站点、FTP 文件下载、网络共享文件及常规的网络通信、盗版软件、示范软件、计算机实验室和其他共享设备。

病毒传播进入系统的途径主要有以下 3 种：

1. 通过计算机网络进行传播

现代信息技术的巨大进步已使空间距离不再遥远，“相隔天涯，如在咫尺”，但也为计算机病毒的传播提供了新的“高速公路”。计算机病毒可以附着在正常文件中，通过网络进入一个又一个系统，尤其服务器是网络的整体或部分核心，一旦其关键文件被感染，再通过服务器的扩散，病毒将会对系统造成巨大的破坏。在信息国际化的同时，病毒也在国际化，国内计算机感染一种“进口”病毒已不再是什么大惊小怪的事了。

这种方式已成为计算机病毒的第一大传播途径。

2. 通过移动存储设备来进行传播

移动存储设备包括软盘、磁带、U 盘、光盘、MP3、MP4 和移动硬盘等。这些设备是使用最广泛、移动最频繁的存储介质，因此也成了计算机病毒寄生的“温床”。

3. 通过通信系统进行传播

通过点对点通信系统和无线通信信道，也可以传播计算机病毒。目前出现的手机病毒，就是利用无线信道进行传播的。

7.3.2 计算机病毒防治管理措施

当病毒影响到社会的正常秩序，危害到国家的安全时，必须有相关的法律法规和管理制度来规范人们的行为，起到威慑作用，并依法追究肇事者的法律责任。早在 1984 年，美国国会就通过了计算机欺骗与滥用法令条文。我国于 1994 年颁布了《中华人民共和国计算机信息系统安全保护条例》，其中规定“故意输入计算机病毒以及其他有害数据，危害计算机信息安全的，要对个人和单位处以高额罚款，并依法追究刑事责任”。1997 年出台的新《刑法》中，增加了有关对制作、传播计算机病毒进行处罚的条款。2000 年 5 月，公安部颁布实施了《计算机病毒防治管理办法》，进一步加强了我国对计算机病毒的预防和控制工作。同时，为了保证计算机病毒防治产品的质量，保护计算机用户的安全，公安部建立了计算机病毒防治产品检验中心，并先后颁布了中华人民共和国公共安全行业标准《DOS 环境下计算机病毒的检测方法》（GA 135—1996）和《计算机病毒防治产品评级准则》（GA 243—2000）。这些法律法规和制度的制定和实施对于规范计算机和网络环境、防范病毒起



到了积极的作用。

除了网络和移动存储设备外，大量的盗版软件和盗版光盘也成为病毒在我国广泛流行的主要载体，计算机软件市场的混乱，软件、游戏的非法复制是病毒泛滥的根源之一。因此，打击盗版，加强软件市场管理不仅是我国精神文明建设的重要内容，而且成为我国防止病毒传播、净化网络和计算机环境的一个重要方面。同时，也要加强计算机安全的教育，宣传计算机病毒的危害，普及预防计算机病毒的基本知识，提高系统管理人员和每个计算机使用人员对病毒的认识和防治的意识；其次，强化管理制度，建立计算机硬件和软件系统的使用、维护、备份和病毒报告等各个环节的安全规章制度；最后，要积极采取各种病毒预防、检测和消除的技术措施。

7.3.3　病毒预防

病毒预防是指根据系统特性，采取相应的系统安全措施预防病毒侵入计算机系统。下面汇总一系列简单有效的措施，以供参考。

计算机病毒都是有一定源头的，之所以能造成广泛的危害，就在于它能进行广泛的传播。因此，对于普通的计算机用户来说，只要平时多注意些，还是可以在一定程度上避免病毒入侵的。

下面将介绍预防计算机病毒应注意的一些事项。

1．使用正版软件

盗版软件是病毒传播的主要渠道，市场上多次转手、来历不明的软件最有可能因缺少检测而成为各种病毒的绝好载体和传染源。

2．从可靠渠道下载软件

目前网上提供有许多免费软件、共享软件，但不要盲目地下载，一定要到有名的大网站（最好是该软件生产商自己的网站）上下载，因为有些无名小网站的免费下载软件很难保证没有被病毒感染。一般情况下，在安装之前要对下载的软件进行病毒扫描，以防万一。

3．安装防病毒软件、防火墙等防病毒工具，准备一套具有查毒、防毒、杀毒及修复系统的工具软件，并定期对软件进行升级、对系统进行查毒

为了防止病毒的入侵，一定要在计算机中安装防病毒软件，并选择公认质量最好、升级服务最及时、能够最迅速有效地响应和跟踪新病毒的防病毒软件。

防病毒软件一般都提供实时监控功能，这样无论是在使用外来软件还是在连接到网络时，都可以先对其进行扫描，如果有病毒，防病毒软件会立即报警。

由于病毒的层出不穷及不断更新，要有效地扫描病毒，防病毒产品就必须适应病毒的发展，及时升级，这样才能保证所安装的防病毒软件中的病毒库是最新的，也只有这样才能识别和杀灭新病毒，为系统提供真正的安全环境。防病毒软件的升级就是因为厂商增加了查杀若干新类型病毒的功能，及时升级将使用户的计算机系统增强对这些病毒的防御

能力。

一般来说，大的生产商现在都能每周更新病毒库，所以在安装防病毒软件时，要选择信誉好的大公司的产品。

防病毒软件的升级可以到防病毒厂商在当地的经销商处进行，也可以自己通过 Internet 连接到防病毒厂商的站点，按照提示逐步完成升级工作。

4. 对电子邮件提高警惕

目前很多具有巨大破坏力的病毒都是通过电子邮件进行传播的，波及范围广、传播速度快，造成的危害也相当大。

大家一般都会对陌生邮件有提防心理，但我们对熟人的邮件也不应该掉以轻心。有些病毒会在入侵到一台计算机后，搜索用户的地址簿，并以该用户的名义向地址簿中的每个地址发送带毒邮件。所以，一定要对电子邮件提高警惕。

其实，邮件本身是纯文本文件，它是不会带毒的，邮件病毒一般都是附着于附件中，所以一定要小心附件，不要打开来历不明的邮件附件。较妥当的做法是先将附件保存下来，经杀毒软件检查后再打开。

5. 经常对系统中的文件进行备份

备份工作应该定期或不定期地进行，确保每一过程和细节的准确、可靠，以便在系统崩溃时最大限度地恢复系统，减少可能出现的损失。

系统数据，例如分区表、DOS 引导扇区等，需要用 BOOT_SAFE 等实用程序或 DEBUG 编程手段做好备份，作为系统维护和修复时的参考。

重要的用户数据，例如有用的文档资料或自己编制的程序文件等，也应当及时备份。

备份时，尽可能地将数据和系统程序分别存放。可以通过比照文件大小、检查文件个数、核对文件名来及时发现病毒。

6. 备好启动盘，并设置写保护

在对计算机系统进行检查、修复和手工杀毒时，通常要使用无毒的启动盘，使设备在较为干净的环境下进行操作。

7. 开机时使用本地硬盘

尽量不用软盘、U 盘、移动硬盘或其他移动存储设备启动计算机，而用本地硬盘启动。

8. 做好系统配置

重要的系统文件和磁盘可以通过赋予只读功能，避免病毒的寄生和入侵。也可以通过转移文件位置，修改相应的系统配置来保护重要的系统文件。

9. 尽量做到专机专用

也就是说，尽量不要让别人使用自己的计算机。尤其是重要部门的计算机，尽量专机专用且与外界隔绝。如果做不到这一点，起码也要保证做到不让别人在自己的机器上使用

曾经在别的机器上使用过的 U 盘等移动存储设备。在万不得已的情况下，也要先进行查毒，在确认无病毒的情况下才可以使用。

同时，应尽量避免在无防病毒措施的机器上使用软盘、U 盘、移动硬盘、可擦写光盘等可移动的存储设备。并且，不要随意借入和借出这些移动存储设备。在使用借入或返还的这些设备时，一定要先使用杀毒软件查毒，避免感染病毒。对返还的设备，若有干净备份，应重新格式化后再使用。

10. 新购置的计算机软件或硬件也要先查毒再使用

新购置的计算机软件和硬件中都可能会携带病毒，因此都需要先进行病毒检测或查杀，证实无病毒后再使用。

虽然在由著名厂商发售的正版软件中也曾经发现了病毒的存在，但总的来说，正版软件还是可靠得多。在 1999 年 4 月 26 日的 CIH 病毒大爆发中，盗版光盘的泛滥对 CIH 病毒的广泛传播起到了非常重要的作用。

新购置的硬盘中也可能会含有病毒。因为对硬盘只做 DOS 的 FORMAT 格式化是不能去除主引导区和分区表扇区中的病毒的，因此可能需要对硬盘进行低级格式化。

11. 使用复杂的密码

有许多网络病毒是通过猜测简单密码的方式攻击系统的，因此使用复杂的密码可大大提高计算机的安全系数。

12. 注意自己的机器最近有无异常

由于在技术上防杀病毒尚无法达到完美的境地，难免有新病毒会突破防护系统的保护，传染到计算机中。因此，为能够及时发现异常情况，不使病毒传染到整个磁盘，传染到相邻的计算机，应对病毒发作时的症状予以注意。

计算机病毒出现什么样的表现症状，是由计算机病毒的设计者决定的。而计算机病毒设计者的思想又是不可判定的，所以计算机病毒的具体表现形式也是不可判定的。然而可以肯定的是，病毒症状是在计算机系统的资源上表现出来的，具体出现哪些异常现象和所感染病毒的种类直接相关。

计算机如果感染了病毒，可能会出现如下一些现象。

（1）屏幕上出现异常图形或画面，这些画面可能是一些鬼怪，也可能是一些下落的雨点、字符、树叶等，并且系统很难退出或恢复。

（2）扬声器发出与正常操作无关的声音，例如演奏乐曲或是随意组合的、杂乱的声音。

（3）磁盘可用空间减少，出现大量坏簇，且坏簇数目不断增多，直到无法继续工作。

（4）磁盘读/写文件明显变慢，访问的时间加长，有时出现“写保护错”提示。

（5）系统经常死机或异常的重启现象增多。

（6）原来正常运行的程序突然不能运行，总是出现出错提示。

（7）文件的大小和修改日期发生变化。

（8）系统的运行速度变得非常缓慢。

（9）用 MI 检查内存时，发现有不应该驻留的程序已经驻留。

（10）键盘、打印或显示有异常现象。

（11）有特殊文件自动生成，或系统的启动速度明显比平时变慢。

（12）莫名其妙地丢失文件。

（13）计算机存储系统的存储容量异常减少，或有不明常驻程序。

（14）系统不能识别磁盘或是硬盘不能开机。

（15）整个目录变成一堆乱码。

（16）硬盘的指示灯无缘无故地亮了。

（17）异常要求用户输入口令。

（18）对贴有写保护的软盘操作时，声音很大。

以上这些现象的出现可能是因为计算机系统感染了病毒，也可能是系统中存在有问题的软件或出现了硬件故障。这时需要立即进行病毒检测，如果发现病毒则要清除，降低病毒对系统的危害程度。

13. 了解一些病毒知识

多了解一些病毒知识，可以及时发现新病毒并采取相应措施，在关键时刻使自己的计算机免受病毒的破坏。例如定期检查注册表中的下列键值：HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run、HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\runservices。

一旦发现病毒，应迅速隔离受感染的计算机，避免病毒继续扩散；并使用可靠的查杀工具进行查杀；必要时需向国家计算机病毒应急中心和当地公共信息网络安全监察部门报告，请专家协助处理。

若硬盘资料已遭破坏，应利用灾后重建的解毒程序和恢复工具加以分析，重建受损状态，而不要急于格式化。

对于计算机病毒的防治，不仅是一个设备的维护问题，而且是一个合理的管理问题；不仅要有完善的规章制度，而且要有健全的管理体制。所以，只有提高认识、加强管理，做到措施到位，才能防患于未然，减少病毒入侵后所造成的损失。

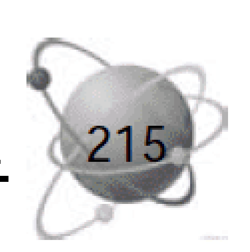
7.3.4 病毒检测

病毒检测就是要在特定的系统环境中，通过各种检测手段来识别病毒，并对可疑的异常情况进行报警。病毒检测主要是通过病毒扫描、系统完整性检查、分析法、校验和法和行为封锁法等 5 种手段进行。

1. 病毒扫描

这是早期使用得较多的一种病毒检测手段。

进行病毒扫描时，必须用未受病毒感染的 DOS 系统软盘启动。只有这样，才能保证内存中没有病毒。某些计算机病毒在内存中时会欺骗检测者。例如前面介绍的“巴基斯坦大



脑”病毒在内存中驻留时，检查引导扇区时看不到病毒程序而只能看到正常的引导扇区。

而且，启动 DOS 系统软盘时必须冷启动，而不能通过按 Ctrl+Alt+Del 键进行热启动。因为某些病毒可以通过截取键盘中断，而将自己仍旧驻留在内存中。

病毒扫描一般通过下面两种方法进行：

（1）将原始备份与检测的对象进行比较

这种方法的优点是使用简单、方便，而且不需要专门的查病毒软件，直接使用常规的 DOS 软件和 PC Tools 等工具软件就可以进行。使用比较法，还可以发现那些尚不能被现有检查病毒程序发现的计算机病毒。

通过比较可以发现异常情况，例如文件长度的变化、程序代码内容的变化等。但对原始备份与检测对象之间的差异不能直接认定是由病毒造成的，尚需专业人员使用反汇编等技术进行进一步分析才能得出结论。

（2）寻找病毒特征

这种病毒扫描软件的开发者首先必须仔细分析各种病毒程序，从中提取出足以代表各种病毒特征的代码串或特征字，建立起病毒特征库。

扫描程序利用该代码库对检测对象进行扫描，如果在检测对象内部或内部的某些特定部位发现了某一特定代码串或特征字，则认为发现了该代码串或特征字所代表的病毒。

显然，病毒特征库中的病毒代码串或特征字种类越多，扫描程序能够识别的病毒也越多。

这种方法在实际应用中，需要不断地将发现的新病毒特征扩充到病毒特征库中，以反映出新病毒的产生或病毒的变异。

这种方法可能会产生“误诊”。如果开发人员选择病毒特征时不够谨慎，可能会将其他正常软件中也有的代码串或特征字包含到病毒代码库中。

这种方法的优点是检测准确、快速，可识别病毒名称和类别，误报警率低，容易对病毒进行清除处理；但缺点是不能检测未知病毒，收集已知病毒的特征代码的费用开销大。

2．系统完整性检查

这种防病毒软件利用病毒行为对文件或系统所产生的影响，即病毒对文件或系统做了些什么，来发现和确定病毒。

系统完整性检查程序首先生成未染毒的“干净”文件和系统的原始状态信息（例如文件长度、日期、时间等），甚至一些更复杂的信息（例如内容摘要等），或者在文件和系统信息中插入一些无害的特殊标记代码，然后监视备份与原始对象之间的差异，用以发现病毒感染的迹象。

这种软件既可以连续工作，例如在每次打开文件时都进行检查，也可以按用户预定方案在指定时机工作。

这种方法的主要缺点是：病毒必须已经对文件或系统进行了破坏，系统完整性检查程序才能发现病毒。因此，如果系统在安装这种软件之前已经感染，或者病毒仍处于潜伏期，则系统完整性检查程序就无能为力了。

此外，这种方法也可能会对某些正常操作产生较多的“误诊”，例如由软件升级或程序

设置的改变而导致的对象变化。

3. 分析法

使用分析法的步骤如下：

（1）确认被观察的磁盘引导扇区和程序中是否含有计算机病毒。

（2）确认计算机病毒的类型，判断其是否是一种新型的计算机病毒。

（3）弄清计算机病毒体的大致结构，提取用于特征识别的字节串或特征字，并将其添加到计算机病毒代码库中，供病毒扫描和识别程序使用。

（4）详细分析计算机病毒代码，为相应的防杀计算机病毒措施制定方案。

要使用分析法检测病毒，除了要具备前面提到的专业知识外，还需要有 DEBUG、PROVIEW 等分析工具软件和专用的试验计算机。因为即使是很熟练的防杀计算机病毒的技术人员使用性能完善的分析软件，也不能保证在短时间内将计算机病毒代码完全分析清楚；而计算机病毒有可能在分析阶段继续传染甚至发作，把软盘、硬盘中的数据完全毁坏掉，这就要求分析工作必须在专门设立的试验计算机上进行。在不具备条件的情况下，不要轻易开始分析工作。很多计算机病毒采用了自加密、反跟踪等技术，使得分析计算机病毒的工作变得很困难和枯燥乏味。特别是某些文件型计算机病毒的代码长度可达 10KB 以上，与系统的层次相关，使详细的剖析工作变得十分复杂。

分析病毒的过程有静态分析和动态分析两类。静态分析是指利用反汇编工具将计算机病毒代码打印成反汇编指令程序清单后进行分析，以便了解计算机病毒分成哪些模块，使用了哪些系统调用，采用了哪些技巧，并将计算机病毒感染文件的过程转为清除该计算机病毒、修复文件的过程，判断哪些代码可用作特征码以及如何防御这种计算机病毒。分析人员具备的素质越高，分析过程越快、理解越深；动态分析则是指利用 DEBUG 等调试工具在内存带毒的情况下，对计算机病毒进行动态跟踪，观察计算机病毒的具体工作过程，以进一步在静态分析的基础上理解计算机病毒的工作原理。在病毒编码比较简单的情况下，动态分析不是必须的。但当计算机病毒采用了较多的技术手段时，必须使用静、动态相结合的分析方法完成整个分析过程。

4. 校验和法

对正常文件的内容，计算其校验和，将该校验和写入此文件或其他文件中保存，在文件使用过程中或使用之前，定期地检查由现有内容算出的校验和与原来保存的校验和是否一致，从而发现文件是否被感染，这种方法称为校验和法。

利用校验和法既能发现已知病毒，也能发现未知病毒，但它不能识别病毒类型和指出病毒名称。由于病毒感染并非文件内容改变的唯一原因，也有可能是正常程序引起的，因此该方法经常会产生误报警，且会影响文件的运行速度。

病毒感染会引起文件内容的变换，但校验和法对文件内容的变化太敏感，且又不能区分正常程序引起的变动，因而频繁报警。用监视文件的校验和来检测病毒不是最好的方法，因为当它遇到已有软件版本更新、密码变更、修改运行参数时都会误报警。

校验和法对隐蔽型病毒无效，因为隐蔽型病毒进入内存后，会自动剥去染毒程序中的

病毒代码，使校验和法受骗，对一个有毒文件能计算出正常的校验和。

使用校验和法检测病毒，通常有如下 3 种方式。

（1）在检测病毒工具中纳入校验和法。计算被查文件的校验和，将结果写入被查文件中或检测工具中，然后进行比较。

（2）在应用程序中，植入校验和法自我检查功能。将文件正常状态的校验和写入文件中，每当应用程序被启动时，比较现行校验和与原校验和值，实现应用程序的自检测。

（3）将校验和检查程序常驻内存。每当启动应用程序时，自动比较应用程序内部或其他文件中预先保存的校验和。

使用校验和法的优点是方法简单，能发现未知病毒，也能发现被查文件的细微变化；缺点是有误报警、不能识别病毒类型和名称、不能对付隐蔽型病毒。

5．行为封锁法

行为封锁型软件采用驻留内存后台工作的方式，监视可能因病毒引起的异常行为。如发现异常行为，便及时报告用户，由用户决定其行为是否继续。此类软件试图阻止任何病毒的异常行为，因此可防止新型未知病毒的传播和破坏。当然，有时被认为的“可疑行为”是正常的，所以出现误报是难免的。

此类技术的进一步发展方向是成为智能探测器。

7.3.5　病毒清除

1．清除方法

预防和发现病毒是非常重要的，但是一旦发现文件或系统已经感染了病毒，显然这时要做的第一件事就是进行杀毒。因为病毒也是程序，所以可以使用多种不同的方法进行杀毒处理，例如使用 DOS 的 DEL 命令，或者使用一个商业化的防病毒软件。

杀毒程序是防病毒软件的一个重要组成部分，也是目前可以利用的主要杀毒工具，其专业杀毒处理功能建立在完全了解某种病毒的工作细节的基础上。

如果系统感染的是引导型病毒，则可以使用像 FDISK 和 SIGH 这样的命令恢复原来的引导扇区，但是这样做的工作量非常大。

对于引导型病毒的删除，关系重大。因为在重新创建引导扇区和主引导记录（Master Boot Record，MBR）时出现的任何错误，不但会导致磁盘分区信息丢失，甚至可能会丢失硬盘上的所有文件，导致系统再也无法被引导了。

目前比较流行的方式是，使用可以不断更新病毒特征库的杀毒软件来清除网络病毒。一般来说，网络版杀毒软件具有对网络病毒进行分析、删除病毒程序并恢复原文件的功能。

对付电子邮件病毒之类的网络病毒，安装实时杀毒软件最为有效。实时杀毒软件会时刻监视用户对外的任何操作，在后台监视操作系统的文件操作。在用户进行磁盘访问、文件复制、文件创建、文件改名、程序执行、系统启动时，自动检测病毒。

现在，许多防病毒软件都采用了实时扫描技术。

网络中的病毒活动状况对于网络管理员来说是非常重要的。通过了解网络中的病毒活动情况，网络管理员可以了解哪些病毒活动比较频繁、哪些计算机或者用户的文件比较容易感染病毒以及病毒的具体特征等，以便修改病毒防范策略以及了解病毒的来源情况，方便进行用户、文件资源的安全管理。

2. 著名杀毒软件公司的站点网址

表 7-3 给出了一些著名杀毒软件公司的站点网址。

表 7-3　著名杀毒软件公司的网址

站点或公司名称	网　　址
冠群金辰	www.kill.com.cn/
瑞星公司	www.rising.com.cn/
北京江民新技术公司	www.jiangmin.com/
信源公司	www.vrv.com.cn/
北京时代先锋（行天 88）	www.sdxf.com/
赛门铁克	www.symantec.com/
McAfee VirusScan	www.mcafee.com/down/downeval.asp/
F-Prot（文件保护神）	www.dataFellows.com/
Dr.solomo's AntiVirus toolkit（所罗门医生）	www.drsolomon.com/

3. 染毒后的紧急处理

当系统感染病毒后，可采取以下措施进行紧急处理，以恢复系统或受损部分。

（1）隔离。当某计算机感染病毒后，可将其与其他计算机进行隔离，即避免相互复制和通信。当网络中某节点感染病毒后，网络管理员必须立即切断该节点与网络的连接，以避免病毒扩散到整个网络。

（2）报警。病毒感染点被隔离后，要立即向网络系统安全管理人员报警。

（3）查毒源。接到报警后，系统安全管理人员可使用相应的防病毒系统鉴别受感染的机器和用户，检查那些经常引起病毒感染的节点和用户，并查找病毒的来源。

（4）采取应对方法和对策。网络系统安全管理人员要对病毒的破坏程度进行分析检查，并根据需要采取有效的病毒清除方法和对策。如果被感染的大部分是系统文件和应用程序文件，且感染程度较深，则可采取重装系统的方法来清除病毒；如果感染的是关键数据文件，或破坏较严重时，可请防病毒专家进行清除病毒和恢复数据的工作。

（5）修复前备份数据。在对病毒进行清除前，尽可能将重要的数据文件备份，以防在使用防病毒软件或其他清除工具查杀病毒时，破坏重要数据文件。

（6）清除病毒。重要数据备份后，运行查杀病毒软件，并对相关系统进行扫描。发现有病毒，立即清除。如果可执行文件中的病毒不能清除，应将其删除，然后再安装相应的程序。

（7）重启和恢复。病毒被清除后，重新启动计算机，再次用防病毒软件检测系统中是

否还有病毒，并将被破坏的数据进行恢复。

7.3.6　病毒防治软件介绍

1. 常用病毒防治软件简介

安装杀毒软件、防火墙等防病毒工具，依靠病毒防治软件对系统进行保护是防止病毒入侵、降低病毒破坏造成的损失所必须的，是防治病毒的主要手段。各种防病毒软件通常具有如下一些功能：按照用户要求对系统进行定期查毒、杀毒；对系统进行文件级、邮件级、内存级、网页级的实时监控；定期或智能化地升级病毒库；硬盘数据的保护、备份和恢复；注册表的维护和修复；多种压缩格式的查毒、杀毒；多种安全策略的选择和用户自定义安全规则的设置。有些还提供了硬盘恢复工具、系统漏洞扫描工具、系统优化工具等。

下面将介绍几种较为流行的防病毒软件。

（1）国际品牌级

① 卡巴斯基。卡巴斯基（Kaspersky）杀毒软件来源于俄罗斯，是世界上最优秀的网络杀毒软件之一，查杀病毒性能较高。该软件具有较强的中心管理和杀毒能力，提供了各种类型的病毒防护解决方案——抗病毒扫描仪、监控器、行为阻断和完整性检验；支持几乎所有的操作系统、E-mail 通路和防火墙，严密控制所有可能的病毒进入端口；其强大的功能和局部的灵活性以及网络管理工具为自动信息搜索、中央安装和病毒防护控制提供了便利。

② 诺顿。Symantec 的诺顿品牌是个人用户安全和解决方案领域的全球零售市场的领导者。它通过无缝集成的产品，保护个人计算机免受病毒爆发或恶意黑客的攻击。全球 500 强企业中的 454 家和《财富》杂志 500 强中的 489 家企业，都在使用 Symantec 解决方案。

③ NOD32。Eset 公司的 NOD32 是全球较为流行的防病毒软件之一，深受用户欢迎。NOD32 在准确度及速度上均打破了多项世界记录。它在全球共获得 40 多个奖项，包括 Virus Bulletin、PC Magazine、ICSA 认证、Checkmark 认证等，并且是全球唯一通过 26 次 VB 100% 测试的防病毒软件。NOD32 提供多种操作系统平台的产品，包括 DOS、Windows 9x/Me、Windows NT/XP/2000、Novell Netware Server、Linux、BSD 等。

（2）国产品牌级

国产防病毒软件占有了国内 80%的市场，其中包括江民 KV 系列、金山毒霸、瑞星杀毒软件、熊猫卫士等一批优秀的品牌。

① 江民 KV 系列。江民科技致力于成为国内最大的信息安全技术开发商与服务提供商，研发和经营范围涉及单机、网络防病毒软件，单机、网络黑客防火墙，邮件服务器防病毒软件等一系列网络安全产品。江民 KV 系列产品在单机版防杀毒市场上占有一定优势，在国内防杀毒业界保持着一定的领先地位。江民系列产品的特点是：与操作系统结合紧密，节约系统资源，不影响系统的稳定性和客户的正常操作；其界面风格简洁，可操作性强，易于使用；在查毒率方面、查杀压缩格式和加壳格式文件的支持方面，江民都表现得很出色。

② 金山毒霸。金山公司是中国领先的应用软件产品和服务供应商，其金山毒霸系列杀毒软件产品是国内较有影响的防杀毒品牌之一。金山公司在积极推广金山毒霸和金山网镖的同时，还积极推动反垃圾邮件活动。金山毒霸的查杀毒速度快是其产品的一大特点；在精细查毒方式下，其查毒率也较高；可以对多种压缩格式进行病毒查杀；在清除病毒方面，金山毒霸也有很好的表现。

③ 瑞星杀毒软件。北京瑞星计算机科技开发有限责任公司是从事计算机病毒防治与研究的专业软件公司，致力于研制、生产涉及计算机防病毒和信息安全相关的系列产品，相继推出了基于多种操作系统的瑞星杀毒软件单机版、网络版、企业级防火墙、入侵检测、漏洞扫描等系列信息安全产品。瑞星杀毒软件具有智能防病毒引擎，对未知病毒、变种病毒、黑客木马、恶意网页程序、间谍程序有快速查杀的能力，并拥有及时便捷的升级服务和技术支持。

④ 熊猫卫士。熊猫卫士是 Panda 软件公司在中国推出的防病毒产品，方正科技于 2002 年初正式入资熊猫中国，成为熊猫软件国内的主要股东，并成为一个拥有核心本土技术的国际化厂商。熊猫卫士可以抵御病毒、蠕虫和特洛伊木马，防护新的网络病毒的攻击，（例如垃圾邮件、间谍程序、拨号器、黑客工具等）。

2. 杀毒软件实例简介

（1）瑞星杀毒软件的安装

安装瑞星杀毒软件的具体步骤如下：

① 下载瑞星杀毒软件的安装程序后，直接执行安装程序，在打开的欢迎界面中单击“下一步”按钮，如图 7-4 所示。

② 进入“最终用户许可协议”界面，阅读协议后必须同意此条款，即选中“我接受”单选按钮，才可以根据安装向导继续进行软件的安装，如图 7-5 所示。

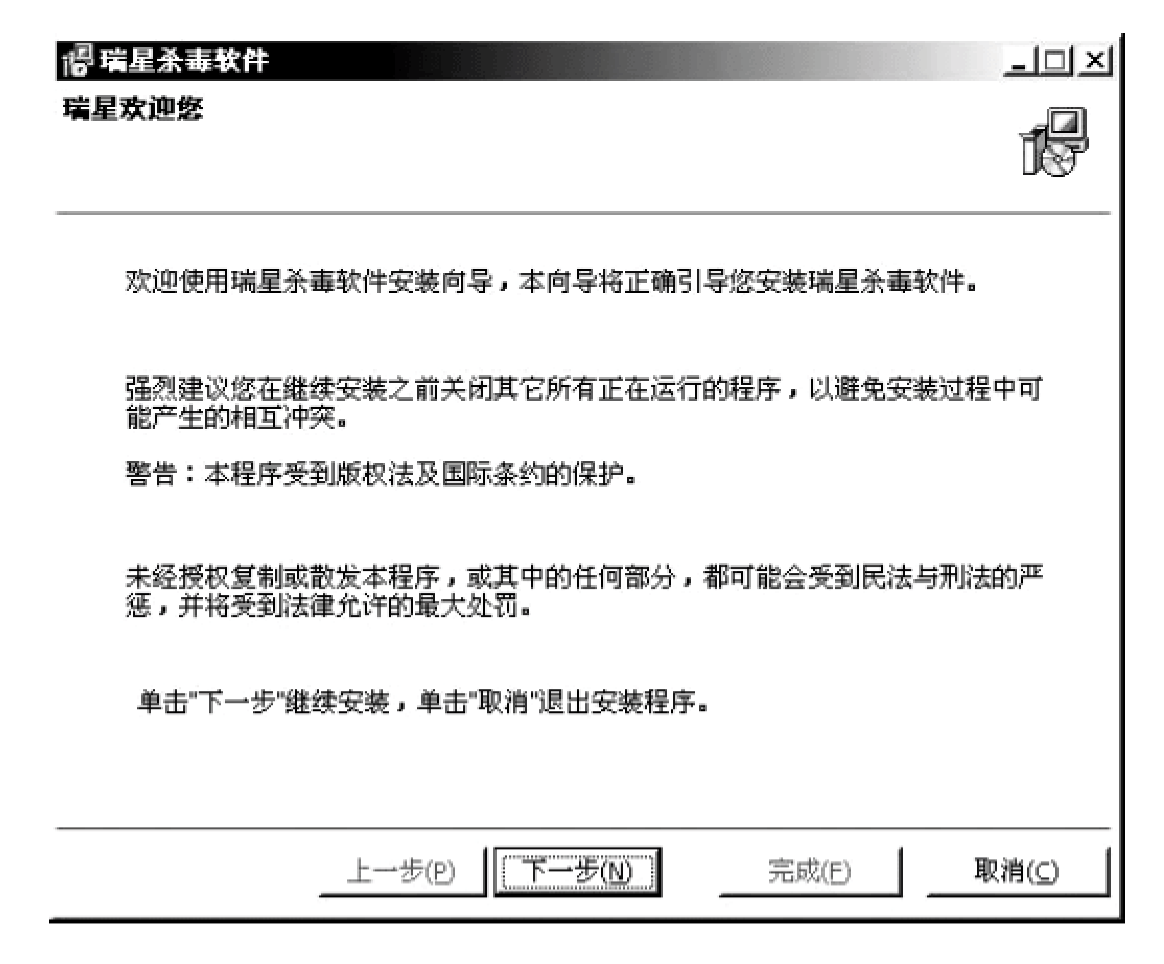



图 7-4 欢迎界面

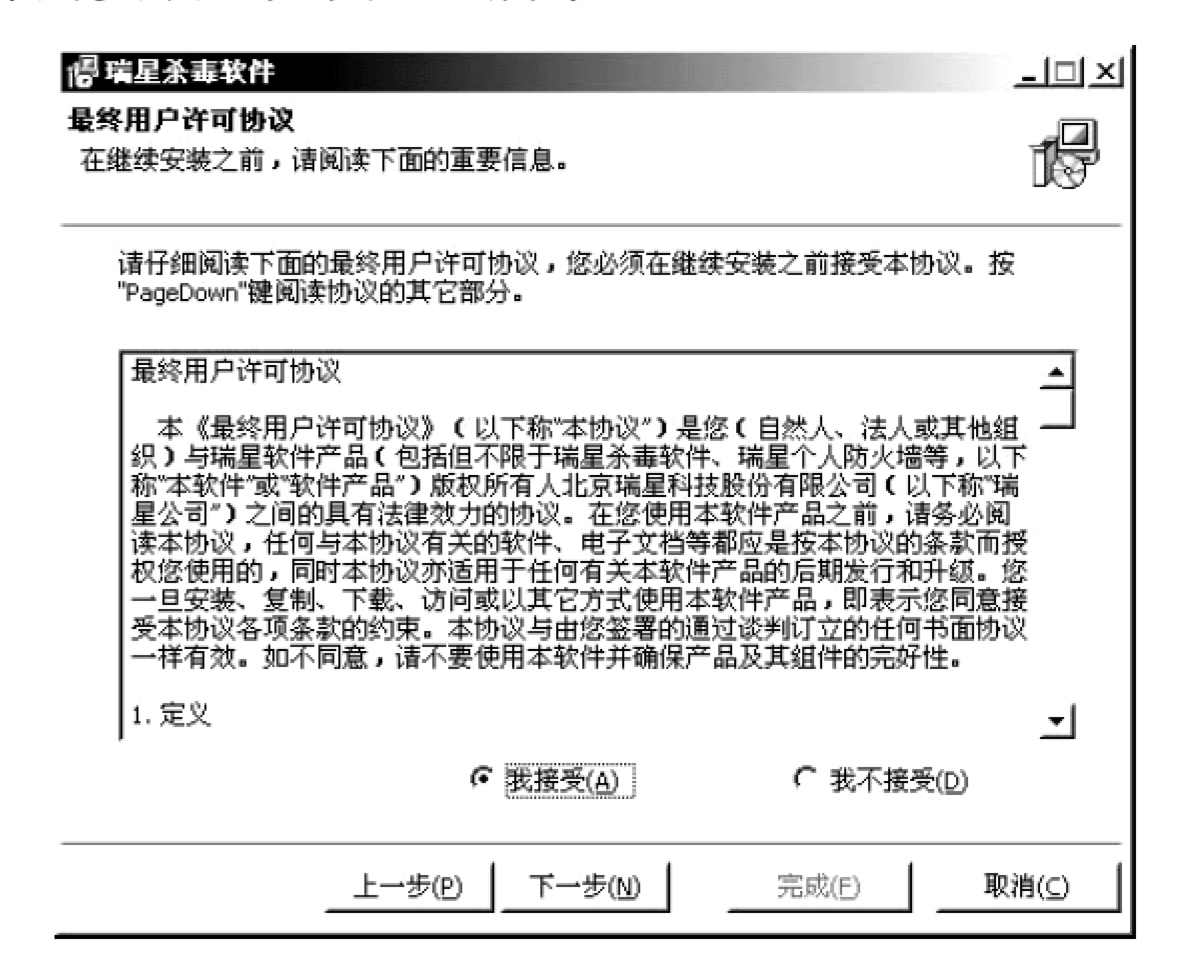


图 7-5 “最终用户许可协议”界面

③ 进入“验证产品序列号和用户 ID”界面，在“产品序列号”框中输入瑞星的产品序列号，同时在“用户 ID”框中输入 12 位用户 ID，如图 7-6 所示。

④ 单击“下一步”按钮，在出现的界面中选择安装方式。瑞星杀毒软件提供了“全部安装”和“最小安装”两种安装方式。

若选择了“全部安装”方式，则可以根据需要选择要安装的其他组件，例如瑞星工具、瑞星皮肤资源等，如图 7-7 所示。

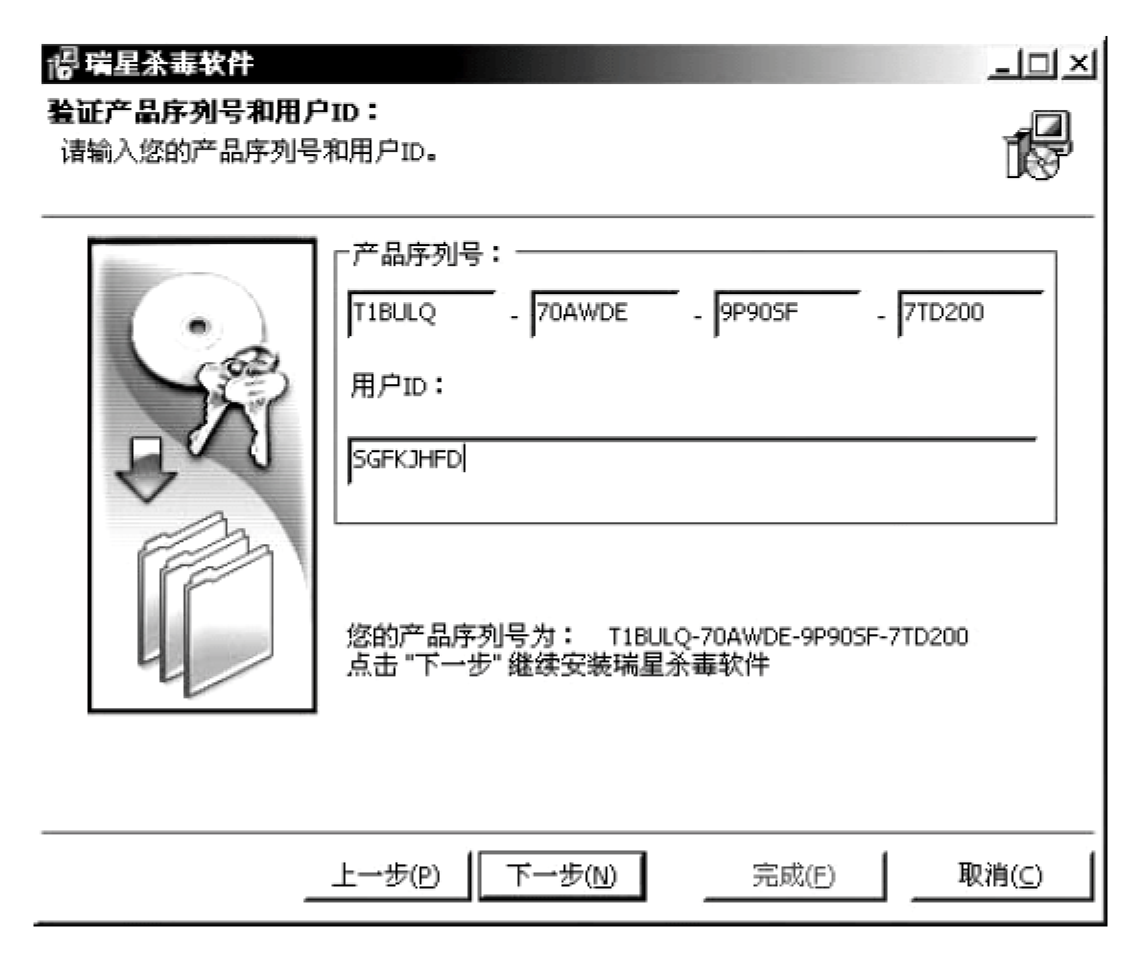


图 7-6　“验证产品序列号和用户 ID”界面

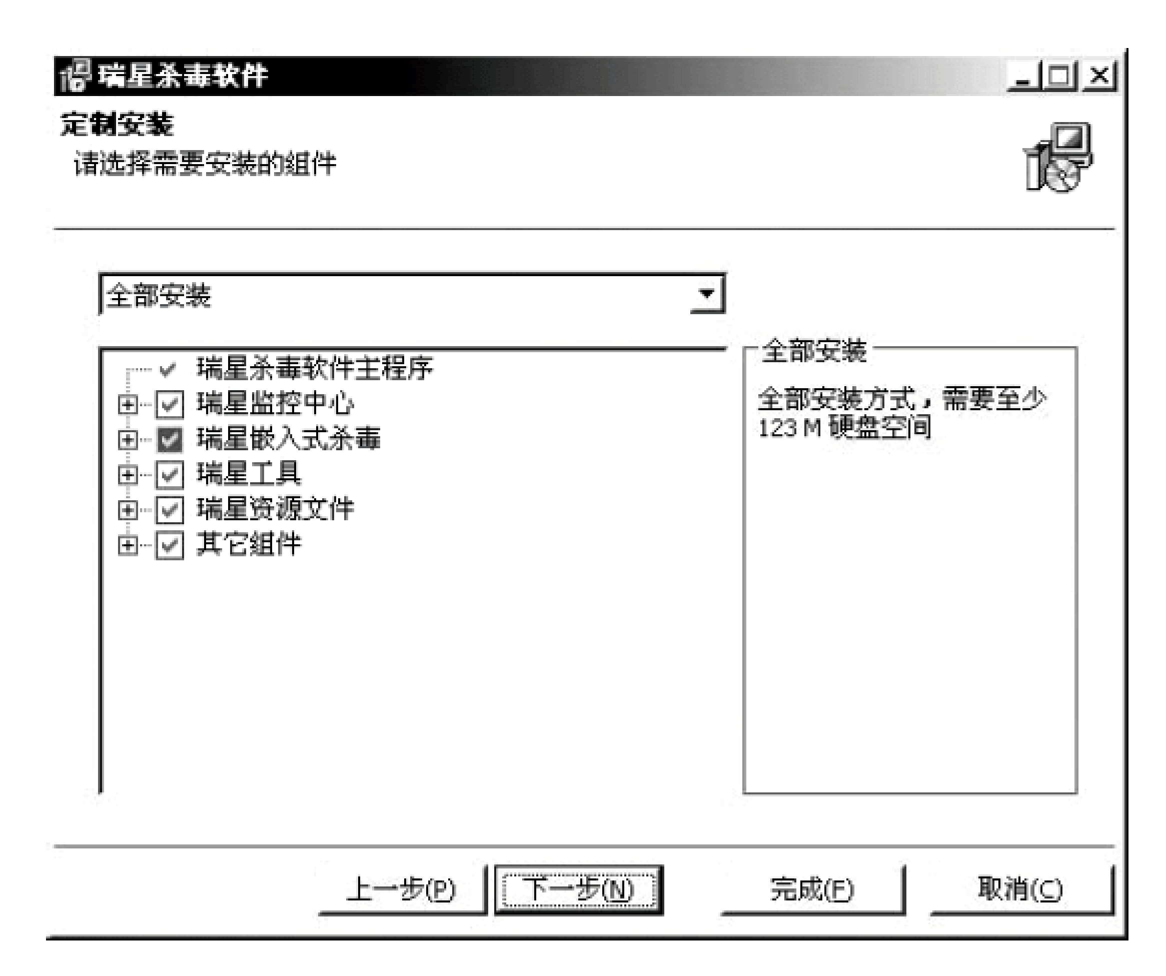


图 7-7　“定制安装”界面

⑤ 单击“下一步”按钮，选择将该软件安装到合适的位置。该软件的默认安装路径是 C:\Program Files\Rising\Rav 文件夹。也可单击“浏览”按钮，在打开的对话框中自行设定安装的路径，如图 7-8 所示。

⑥ 单击“下一步”按钮，选择瑞星防火墙在系统“开始”菜单中的文件夹，以便用户可方便地通过“开始”菜单启动防火墙，并确定是否放置瑞星图标到桌面和是否放置瑞星图标到快速启动工具条，如图 7-9 所示。

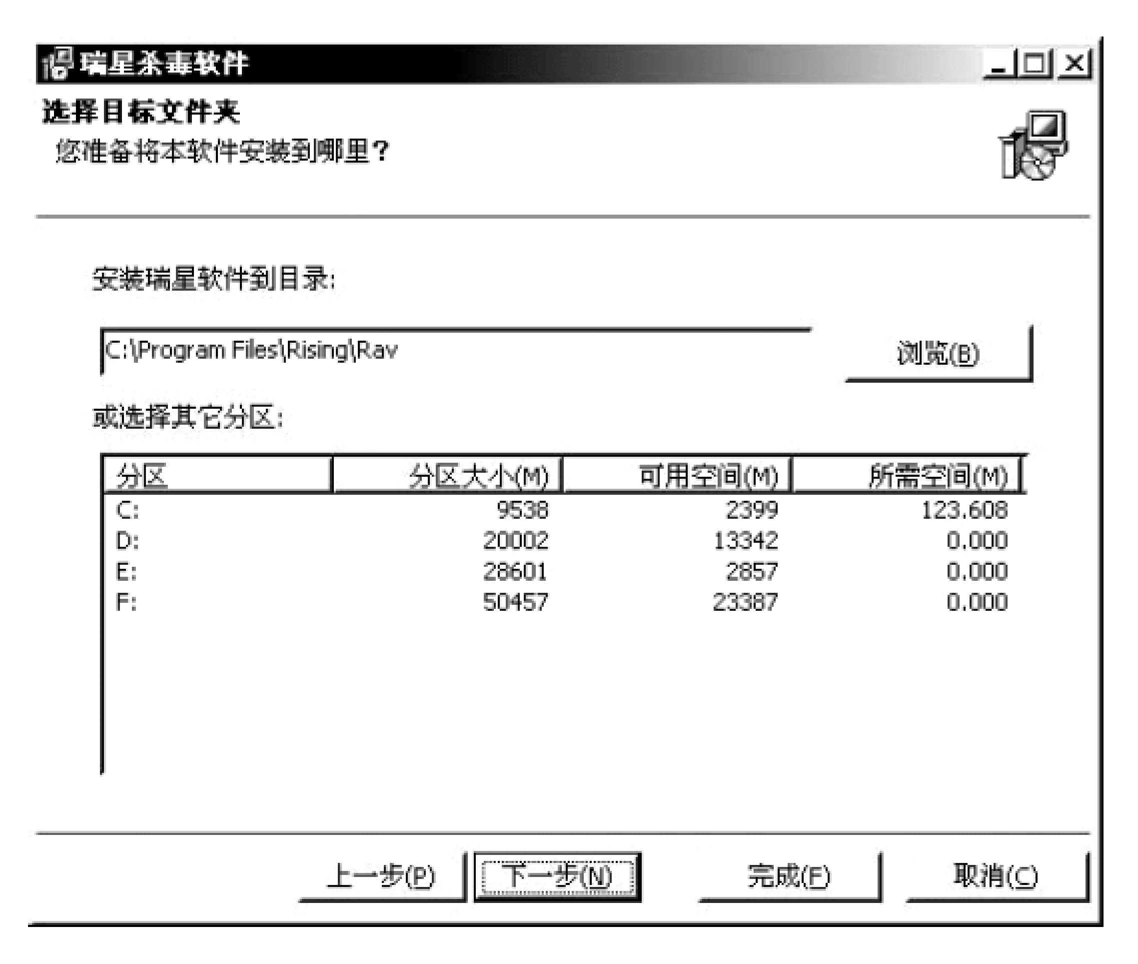


图 7-8　“选择目标文件夹”界面

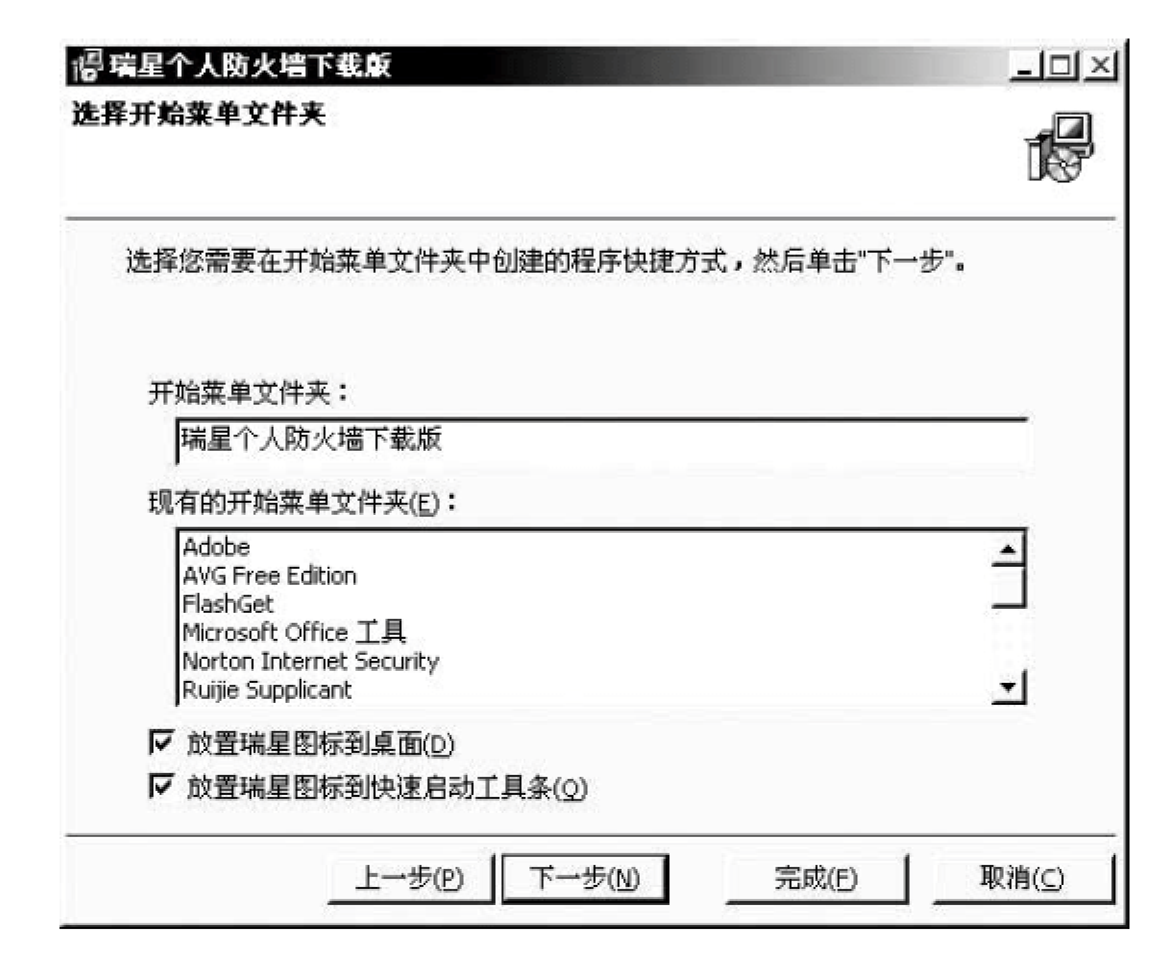


图 7-9　“选择开始菜单文件夹”界面

⑦ 单击“下一步”按钮，进入“安装过程中”界面，此时将进行文件的复制和安装，如图 7-10 所示。



图 7-10 “安装过程中”界面

⑧ 完成瑞星杀毒软件安装后，进入“结束”界面，如图 7-11 所示。单击“完成”按钮，瑞星杀毒软件就安装到计算机上了。在任务栏的右侧，将会出现瑞星杀毒软件的图标。

（2）瑞星杀毒软件的卸载

瑞星杀毒软件提供了自动卸载程序，卸载方法如下：

① 在弹出的菜单中选择“程序”命令，找到瑞星杀毒软件的安装目录，选择“添加删除组件”命令，如图 7-12 所示。





图 7-11 “结束”界面



图 7-12 选择“添加删除组件”命令

② 打开“瑞星软件维护模式”界面，选中“卸载”单选按钮，单击“下一步”按钮，即可完成瑞星杀毒软件的卸载，如图 7-13 所示。

当然，也可以通过控制面板中的“添加或删除程序”功能进行卸载。

（3）瑞星杀毒软件的使用

下面介绍使用瑞星杀毒软件进行杀毒的方法。

① 打开瑞星杀毒软件，将出现如图 7-14 所示的用户界面。在“信息中心”选项卡下，选择要进行查杀毒的对象，如驱动器、内存等，例如要对 E 盘进行杀毒，则选中 E 盘前的

复选框，如图 7-15 所示。

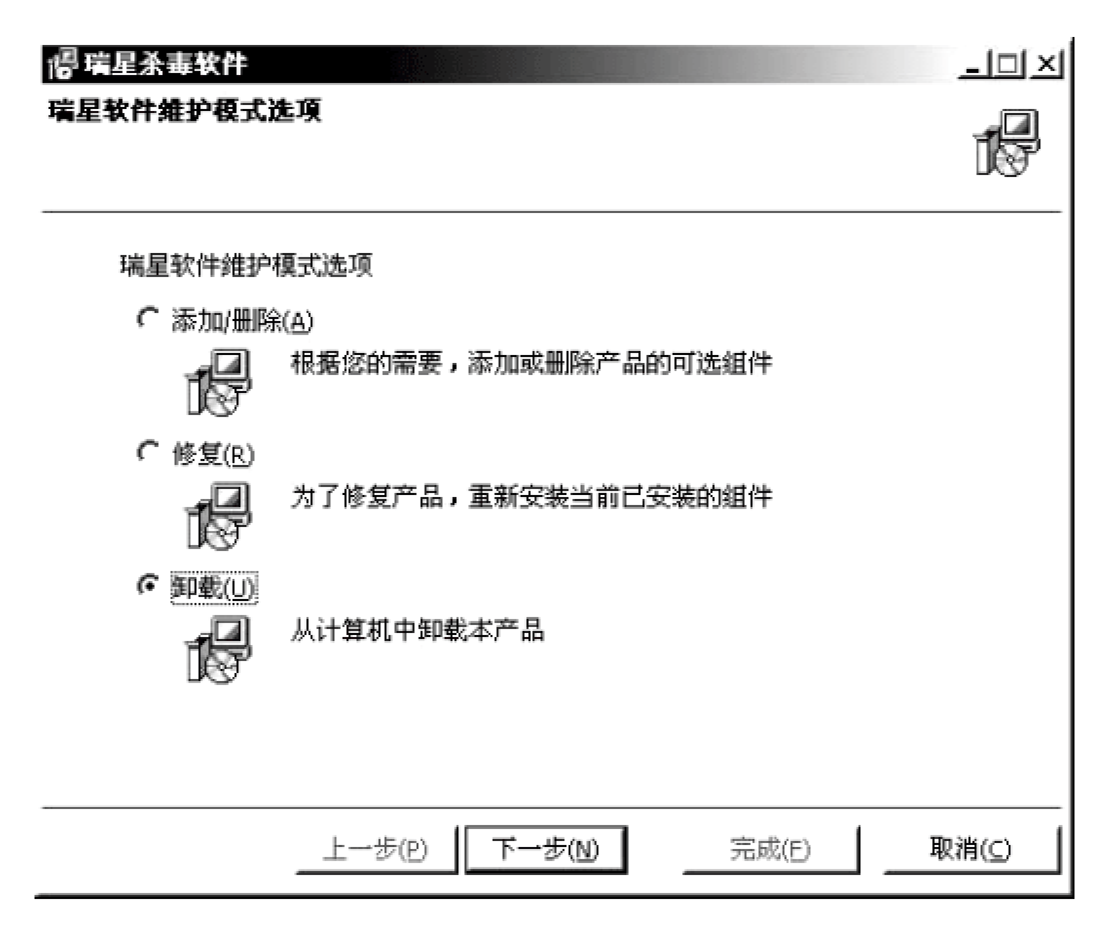


图 7-13　“瑞星软件维护模式”界面



图 7-14　瑞星杀毒软件用户界面



图 7-15　瑞星杀毒软件查杀毒对象选择界面

② 单击屏幕下方的“杀毒”按钮，将出现如图 7-16 所示的杀毒界面。

③ 在杀毒过程中，单击“暂停”按钮可暂停杀毒，单击“停止”按钮可以结束查杀毒。在这些按钮的上方有一个状态显示条，显示了查杀毒的进度。

在最下方的状态栏上，将显示当前已经查杀毒的文件数目以及发现的病毒数目，并显示当前正在查杀毒的具体文件路径。

④ 杀毒完成后，出现如图 7-17 所示的“杀毒结束”对话框，其中详细列出了查杀毒的统计情况。例如，查杀毒的文件数目、用时；如果发现了病毒，则将发现的病毒以及清除情况都反映出来。

另外，也可以在“我的电脑”窗口或资源管理器中选中要进行查杀毒的对象，如 E 盘；然后右击，在弹出的快捷菜单中选择“瑞星杀毒”命令，如图 7-18 所示，即可进入到如

图 7-16 所示的杀毒工作状态中。



图 7-16　瑞星杀毒软件的杀毒工作界面

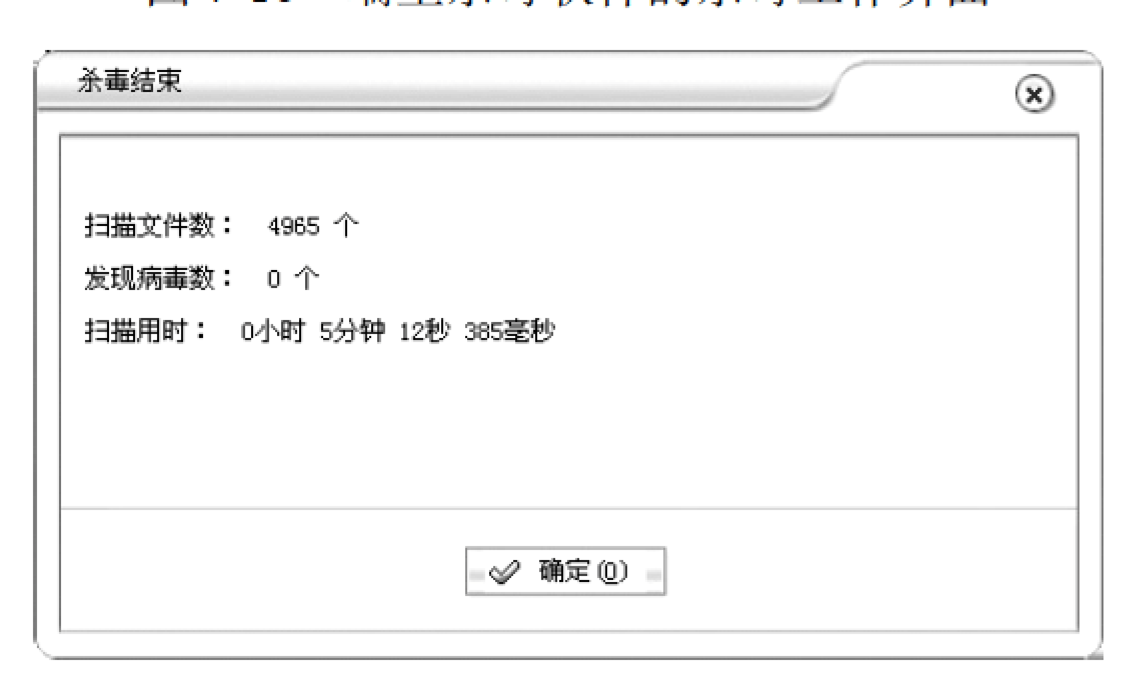


图 7-17　“杀毒结束”对话框

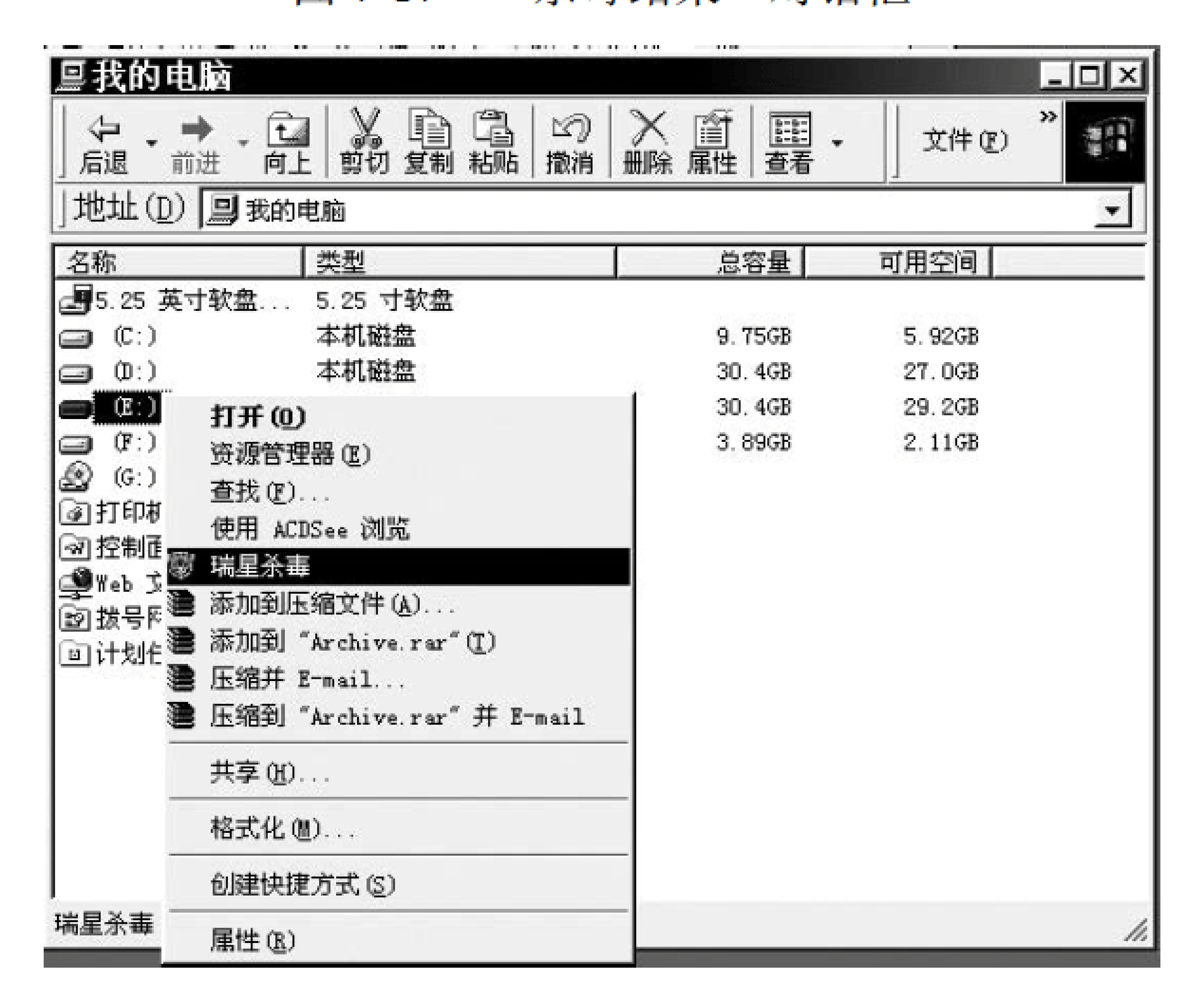


图 7-18　在“我的电脑”中直接查杀病毒

（4）瑞星杀毒软件的升级

在主界面中单击“升级”按钮，并保证计算机与 Internet 互联，就可以对瑞星杀毒软件进行在线升级，将出现如图 7-19 所示的升级界面，直至完成。



图 7-19　瑞星杀毒软件在线升级界面

7.4　典型计算机病毒的检测与清除

7.4.1　网络病毒的检测与清除方法

计算机网络病毒实际上是一个笼统的概念。一种情况是，计算机网络病毒专指在网络上传播并对网络进行破坏的病毒；另一种情况是，计算机网络病毒指的是 HTML 病毒、E-mail 病毒、Java 病毒等与 Internet 有关的病毒。

1．网络病毒的传播方式

事实上，并不是所有的病毒都能够通过计算机网络进行传播。例如，单纯的引导型病毒就很少能在互联网上传播。计算机网络上的病毒几乎都是常规单机病毒，真正能够称得上网络型的病毒很少。也就是说，计算机网络上的病毒机制不过就是单机型的，只不过是通过网络进行传播罢了。这也说明，病毒的传播和感染也由以软盘、软件为媒介发展到互联网时代的以网络（电子邮件等）为媒介。

网络病毒的出现和传播成为当前影响 Internet 正常运转的主要障碍。网络病毒首先来自于文件下载。被浏览的文件和通过 FTP 下载的文件中可能存在病毒，而共享软件和免费的资料已经成为病毒传播的重要途径。

网络病毒的另一种重要来源是电子邮件。大多数的 Internet 邮件系统提供了在网络间传送附件的功能，而病毒恰好抓住了这一点，利用邮件系统的漏洞自动地向邮箱服务器地址列表中的地址发送带病毒的邮件，使病毒得到迅速传播。

随着即时聊天工具的流行，通过聊天工具进行病毒传播成为网络病毒传播的第三大途径。

蠕虫病毒则是利用系统漏洞进行传播的一种网络病毒。

2．网络病毒的特点

计算机网络的主要特点是资源共享，一旦共享资源感染上病毒，网络各节点间信息的频繁传输将把病毒传染到共享的所有机器上，从而形成多种共享资源的交叉感染。病毒的迅速传播、再生、发作将造成比单机病毒更大的危害。

在网络环境中，网络病毒除了具有可传播性、可执行性、破坏性、可触发性等计算机病毒的共性外，还具有如下一些新特点。

（1）感染速度快。在单机环境下，病毒只能通过软盘从一台计算机带到另一台，而在网络中则可以通过网络通信机制迅速扩散。根据测定，一个典型的局域网在正常使用的情况下，只要有一台工作站有病毒，短短几十分钟即可使网上的数百台计算机全部感染。

（2）扩散面广。由于病毒在网络中的扩散非常快，扩散范围很大，不但能迅速传染局域网络内所有计算机，还能通过远程工作站在一瞬间将病毒传播到千里之外。

（3）传播的形式复杂多样。病毒在计算机网络上通过共享文件、电子邮件、文件传送等途径进行传播，其传播的形式可以多种多样。

（4）难以彻底清除。单机上的计算机病毒有时可通过删除带毒文件、低级格式化硬盘等措施将病毒彻底清除，而网络中只要有一台工作站未能干净地杀毒就可使整个网络重新被病毒感染，甚至刚刚完成杀毒工作的一台工作站很可能被网上另一台带毒工作站所感染。因此，仅对工作站进行病毒查杀，并不能解决病毒对网络的危害。

（5）破坏性大。网络病毒破坏力更强，轻则降低速度，影响工作效率，重则使网络崩溃，破坏服务器信息，使多年工作毁于一旦。

3．网络防病毒技术

目前成熟的防病毒软件已经可以做到对所有的已知病毒进行预防和清除，例如瑞星、KV、KILL、诺顿、金山毒霸等。

下面介绍两种网络防病毒技术。

（1）实时监视技术

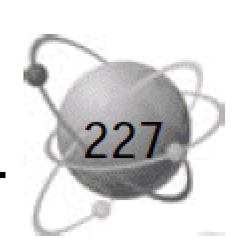
实时监视技术为计算机构筑起一道动态、实时的防病毒防线，它通过修改操作系统，使操作系统本身具备防病毒功能，拒病毒于计算机系统之外。该技术可时刻监视系统中的病毒活动、系统状况以及软盘、光盘、互联网、电子邮件上的病毒传染，将病毒阻止在操作系统外部。

采用实时监视技术的防病毒软件由于使用了与操作系统底层的无缝连接技术，实时监视器占用的系统资源极小，用户完全感觉不到对机器性能的影响。

只要实时防病毒软件实时地在系统中工作，病毒就无法侵入计算机网络系统。防病毒软件只需一次安装，就可保证此后计算机运行的每一秒钟都会执行严格的防病毒检查，保证从 Internet、光盘、软盘等途径进入网络的每一个文件都安全无毒，如有病毒则自动清除。

（2）全平台防病毒技术

目前病毒活跃的平台有 DOS、Windows、Windows NT、NetWare、Exchange 等。为了



使防病毒软件做到与系统的底层无缝连接，实时地检查和清除病毒，必须在不同的平台上使用相应平台的防病毒软件。假如使用 Windows 平台，则必须用 Windows 版本的防病毒软件。如果是企业网络，各种版本的平台都有，那么就要在网络上的每一个服务器、客户端上安装 DOS、Windows XP/NT 等平台的防病毒软件，做到每一个点上都安装相应的防病毒模块，每一个点上都能实时地抵御病毒的攻击。只有这样，才能做到网络的真正安全和可靠。

4. 网络病毒的防治

网络病毒的防治工作具有如下特点。

（1）网络防病毒技术的安全度是基于“木桶理论”的。被计算机安全界广泛采用的著名的“木桶理论”认为，整个系统的安全防护能力取决于系统中安全防护能力最薄弱的环节。计算机网络病毒防治是计算机安全极为重要的一个方面，它同样也适用于这一理论，即一个计算机网络对病毒的防御能力取决于网络中病毒防护能力最薄弱的一个节点。

（2）网络防病毒技术尤其是网络病毒实时监测技术应符合“最小占用”原则。网络防病毒技术的应用必然会占用网络系统资源（增加网络负荷、额外占用 CPU、占用服务器内存等）。网络防病毒产品是网络应用的辅助产品，因此网络防病毒技术，尤其是网络病毒实时监测技术，在自身的运行中不应影响网络的正常运行。因此，网络防病毒技术应符合“最小占用”原则，以保证网络防病毒组件和网络本身都能发挥出应有的正常功效。

（3）网络防病毒技术的兼容性是网络防病毒的重点与难点。网络上集成了那么多的硬件和软件，流行的网络操作系统也有好几种。按照一定网络防病毒技术开发出来的网络防病毒产品，要运行于这么多的软、硬件之上，与它们和平共处，实在是非常之难，远比单机防病毒产品复杂。这既是网络防病毒技术必须面对的难点，又是其必须解决的重点。

5. 网络病毒检测与清除的方法举例

网络病毒的检测与清除，主要依赖于防病毒软件和防火墙的安装。也可以通过如下一些方法，检查系统是否感染了网络病毒。

（1）检查注册表。大多数病毒都会修改注册表，使得每一次机器启动时都能够得到自动执行。常见的被修改的注册表键值存放在：

- HKEY_CURRENT_USERS\software\microsoft\windows\currentversion 下的 run 或 runonce 项下。
- HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion 下的 run、runonceex、runservices 项下。
- HKEY_USERS.DEFAULT\software\microsoft\windows\currentversion 下的 run 或 runonce 项下。

有些病毒为了隐蔽自己，通过修改注册表将自己伪装成系统文件。例如，木马病毒 Acid Battery V1.0 将注册表 HKEY_LOCALMACHINE\software\microsoft\windows\currentversion\run 项下的 Explorer 键值改为 Explorer=“C:\WINDOWS\ EXPIORER.EXE”，病毒程序与真

正的 Explorer 之间只有“i”与“l”的差别。

（2）检查磁盘文件。有些网络病毒会在磁盘上留下自己的文件，例如木马病毒 Netbus；有些修改或覆盖原有系统的文件，例如外壳型病毒；有些则以系统文件的命名方式来命名自己，以迷惑用户。

（3）检查共享文件夹。为实现远程访问的目的，病毒通常将服务程序放在共享目录中。

（4）检查进程。网络病毒在发作时会占用系统资源，自动产生正常系统运行时没有的进程，甚至关闭一些正常系统运行的进程。

（5）检查端口。网络病毒要与外界进行联系或传播病毒，必然要开启通信端口，自动发送垃圾信息，感染其他系统或接受远程控制，窃取系统资料。

（6）其他异常症状。例如，系统性能下降、浏览器被修改、出现乱码、无法正常使用邮件系统等。

不同网络病毒的清除方法各不相同，但大多要涉及到注册表的修改、系统程序的恢复和病毒服务程序的删除。

6. 网络病毒实例——电子邮件病毒

“电子邮件病毒”其实和普通的计算机病毒一样，只不过由于它们的传播途径主要是通过电子邮件，所以才被称为“电子邮件病毒”。现今电子邮件已被广泛使用，E-mail 也成为病毒传播的主要途径之一。由于可同时向一群用户或整个计算机系统发送电子邮件，一旦一个信息点被感染，整个系统在短时间内都可能被感染。

（1）电子邮件病毒的特点

① 邮件格式不统一，杀毒困难。不同的邮件系统使用不同的格式存储文件和文档，传统的杀毒软件对侦测此类格式的文件无能为力。另外，普通用户并不能访问邮件数据库，因为它们往往在远程服务器上。

② 传播速度快，传播范围广，破坏力大。绝大多数通过 E-mail 传播的病毒都有自我复制的能力，而这正是电子邮件病毒的危险之处。电子邮件病毒能够主动选择用户邮箱地址簿中的地址发送邮件或在用户发送邮件时，将被病毒感染的文件附到邮件上一起发送。这种成指数增长的传播速度可以使病毒在很短的时间内遍布整个 Internet。2000 年 5 月 4 日，“爱虫”病毒爆发的第一天便有 6 万台以上的机器被感染，在短短不到一个月的时间内就造成了超过 67 亿美元的损失。当电子邮件病毒发作时，往往会造成整个网络的瘫痪，而网络瘫痪造成的损失往往是难以估计的。

（2）电子邮件病毒的防范措施

电子邮件病毒一般是通过在邮件中“附件”夹带的方法进行扩散，无论是文件型病毒或是引导型病毒，无论是“爱虫”还是“美丽莎”，如果用户没有运行或打开附件，病毒是不会被激活的（Bubbleboy 除外）；只有运行了该附件中的病毒程序，才能使计算机染毒。

对于 E-mail 用户而言，杀毒不如防毒。知道了这一点，对电子邮件病毒就可以从下面几个方面采取相应的防范措施了。



① 不要轻易打开陌生人来信中的附件文件，尤其对于一些“.exe”之类的可执行程序文件，更要慎之又慎！

② 对于比较熟悉、了解的朋友寄来的信件，如果其信中夹带了程序附件，但是他却没有在信中提及或是说明，也不要轻易运行。因为有些病毒是偷偷地附着上去的，也许发送电子邮件的计算机已经染毒，可朋友自己却不知道。例如，Happy 99 就是这样的病毒，它会自我复制，跟着发送的邮件走。

③ 给别人发送程序文件甚至包括电子贺卡时，一定要先在自己的计算机中试试，确认没有问题后再发，以免好心办了坏事。另外，切忌盲目转发。有的用户当收到某些自认为有趣的邮件时，还来不及细看就打开通讯簿给自己的每一位朋友都转发一份，这极有可能使用户无意中成了病毒传播者。

④ 不断完善“网关”软件及病毒防火墙软件，加强对整个网络入口点的防范。

⑤ 使用优秀的防病毒软件对电子邮件进行专门的保护。选用的防病毒软件首先必须有能力发现并杀灭任何类型的病毒，无论这些病毒是隐藏在邮件文本内，还是躲在附件或 OLE 文档内。当然，有能力扫描压缩文件也是必须的。其次，该防病毒软件还必须在收到邮件的同时对该邮件进行病毒扫描，并在每次打开、保存和发送后再次进行扫描。

⑥ 使用防病毒软件同时保护客户机和服务器。一方面，只有客户机的防病毒软件才能访问个人目录，并且防止病毒从外部入侵；另一方面，只有服务器的防病毒软件才能进行全局监测和查杀病毒。这是防止病毒在整个系统中扩散的唯一途径，也是阻止病毒入侵没有本地保护但连接到邮件系统的计算机的唯一方法。

⑦ 使用特定的 SMTP 杀毒软件。SMTP 杀毒软件具有独特的功能，它能在那些从互联网上下载的受染邮件到达本地邮件服务器之前拦截它们，从而保持本地网络的无毒状态。

7.4.2　宏病毒的检测与清除方法

宏是软件设计者为了在使用软件工作时，避免一再重复相同的动作而设计出来的一种工具。在 Word 中，宏是一系列组合在一起的 Word 命令和指令，它们形成了一个命令，可实现任务执行的自动化，代替人工进行一系列费时而单调的重复性 Word 操作，自动完成所需任务。宏病毒是利用软件所支持的宏命令编写而成的具有复制、传染能力的宏。

1. 宏病毒的检测

由于宏病毒在运行时离不开运行它的软件平台 Word、PowerPoint 等 Office 软件，所以通过操作系统和 Office 软件平台的异常现象，就能准确地反映出宏病毒的存在。

（1）检查通用模板中出现的宏。大多数宏病毒是通过感染通用模板 Normal.dot 进行传播的，而通常通用模板中是没有宏的，因此选择“工具”|“宏”命令，如果发现有 Auto Open 等自动宏、File Save 等标准宏或一些怪名字的宏，而用户又没有使用特殊宏的时候，用户文档便很有可能感染上了宏病毒。

（2）无故出现存盘操作。当打开一个 Word 文档时，并且文档没有经过任何改动，立

刻就有存盘操作。

（3）Word 功能混乱，无法使用。宏病毒能够破坏 Word 的运行机制，使文档的打开、关闭、存盘等操作无法正常进行。例如，Word 的.doc 文件无法另存为其他格式的文件，而只能以模板文件方式存盘。

（4）Word 菜单命令消失。一些病毒感染系统时，会关闭 Word 菜单的某些命令，以隐藏和保护自己。例如，Phardera 病毒在其发作时只弹出一个对话框，干扰用户的正常操作，而有的病毒会去掉“工具”菜单中的“宏”和“自定义”命令，阻止手工查杀病毒。

（5）Word 文档的内容发生变化。例如，Wazzu 病毒感染文档后，会打乱原格式，并在文档中加入 Wazzu；Concep.F 病毒则将原文档中的“，”、e、not 替换为“。”、a、and。

2. Word 宏病毒的防范

对于 Word 宏病毒的防范，要注意以下几点。

（1）对于已染病毒的 Normal.dot 文件，应先将 Normal.dot 中的自动宏清除，然后将 Normal.dot 设置成只读方式。

（2）对于其他已感染病毒的文件均应将自动宏清除，这样就可以达到清除病毒的目的。

（3）平时使用时要加强防范：定期检查活动宏表，对来历不明的宏最好予以删除；如果发现后缀为.doc 的文件变成模板（.dot）时，则可怀疑其已感染宏病毒，其主要表现是在 Save As 文档时，选择文件类型的下拉列表框变为灰色。

（4）在启动 Word、创建文档、打开文档、关闭文档以及退出 Word 时，按住 Shift 键可以阻止自动宏的运行。例如，当用含有 AutoNew 宏的模板新建一文档时，在“新建”对话框中单击“确定”按钮时按住 Shift 键，就可以阻止 AutoNew 宏的执行。

（5）存储一个文档时，务必明确指定该文档的扩展名。宏病毒总是试图把模板文件的扩展名加到用户指定的文件名后面，无论扩展名是否已经存在。例如，用户指定文件名为 test.doc，最终这个文件名会变为 test.doc.dot，显然这个文件名在 DOS 下是不可接受的。由此就可以察觉到宏病毒的存在。

3. Word 宏病毒的清除

对于 Word 宏病毒，最简单的清除步骤如下。

（1）在没打开任何文件（文档文件或模板文件）的情况下，启动 Word。

（2）选择“工具”|“模板和加载项”命令，打开“模板和加载项”对话框，单击“管理器”按钮，打开“管理器”对话框。

（3）选择“宏方案项”选项卡，删除左右两个列表框中除了自己定义之外的所有宏，单击“关闭”按钮关闭对话框。

（4）选择“工具”|“宏”命令，若有 AutoOpen、AutoNew、AutoClose 等宏，则删除。

以上步骤，可清除 Word 系统中的宏病毒。

由于 Word 宏病毒会寄生在任何.doc 文档中，可在打开.doc 文件后，重复上面步骤（2）～（4），然后将文件存盘，以清除.doc 文档中的病毒。



7.5　计算机病毒的现状和发展趋势

7.5.1　计算机病毒的现状

2004 年 6 月，手机病毒 Cabir 被发现，并在欧洲掀起了波澜。随后，瑞星在 8 月截获了“布若达”（backdoor.wince.brador.a）病毒，手机病毒开始引起人们的广泛关注。

手机病毒主要是通过短信、下载文件、红外、蓝牙等无线网络连接方式进行传播。而手机同样会因为中了病毒而出现死机、电话簿丢失等意外情况；此外，还会对各种移动设备产生类似的破坏作用。2004 年利用手机无线传送功能传播的病毒同比增加了 80%，通过手机操作系统扩散的病毒增加了 25%，利用短信、彩信传播的手机病毒增加了 48%。

手机病毒与传统计算机病毒的区别在于：手机病毒利用了手机的无线扩展功能进行传播，而计算机病毒则是利用了电子邮件、浏览网页、即时通信等进行传播。同时，手机病毒与计算机病毒又有着很大的联系，它们同属于计算机病毒。可以说，计算机是智能手机病毒扩散的源头，任何手机病毒都要通过计算机进行编写。

2005 年 7 月 13 日，国内最大的防病毒软件厂商江民科技发布了《2005 上半年十大病毒排行》及《中国大陆地区计算机病毒疫情报告及未来发展趋势分析》。报告显示，2005 年上半年度中国大陆地区通过即时通信工具（主要是 QQ 和 MSN）进行传播的病毒已经取代电子邮件成为病毒传播的主流途径，在 2005 年上半年十大恶性病毒排行榜中，与即时通信工具 QQ 和 MSN 有关的病毒占据了一半。2005 年上半年出现的病毒中，木马最为活跃，并且十大病毒排行中木马已经超越蠕虫成为新霸主。

7.5.2　计算机病毒的发展趋势

现在的计算机病毒已经由从前的单一传播、单种行为变成依赖于 Internet 传播，集电子邮件、文件传染等多种传播方式，融木马、黑客等多种攻击手段于一身，形成一种广义的“新病毒”。根据这些病毒的发展演变，可预见未来计算机病毒的更新换代将向多元化方向发展，可能具有如下发展趋势。

1．病毒的网络化

病毒与 Internet 和 Intranet 更紧密地结合，利用 Internet 上一切可以利用的方式进行传播，如电子邮件、局域网、远程管理、即时通信工具等。

2．病毒功能的综合化

利用系统漏洞，成为病毒有力的攻击方式。新型病毒集文件传染、蠕虫、木马、黑客程序特点于一身，破坏性大大加强。

随着时间的不断向前推进，黑客攻击技术和病毒技术都在不断发展进步，两者相互融

合的趋势也更加明显。2003 年流行的“冲击波”、2004 年流行的“震荡波”都属于同一类型的混合型威胁。它们既具有传统蠕虫病毒的“自身复制、修改注册表、向外扩散感染其他主机”特点，又具有传统黑客攻击手段的“根据操作系统某一漏洞发起主动攻击”特征。

病毒和黑客结合，将给信息社会带来更大的危害。融合黑客技术与病毒技术于一身的“新一代主动式恶意代码”，可在极短的时间内，利用优化扫描的方法，感染数以万计的、有漏洞的计算机系统；同时，还能确定并记录用户是否被感染，分析掌握受害者信息，为持续的攻击建立畅通的渠道，进而实施更为恶劣的破坏行为。例如，黑客借助于病毒广泛和迅速传播的特性，把黑客攻击手段从以前的一对一攻击变成了一对多攻击模式。

3. 传播途径的多样化

病毒通过网络共享、网络漏洞、网络浏览、电子邮件、即时通信软件等途径进行传播。

4. 病毒的多平台化

目前，各种常用的操作系统平台病毒均已出现，第一个跨 Windows 和 Linux 平台的病毒 Winux 也于 2001 年 3 月出现，跨各种新型平台的病毒也陆续推出和普及。

手机和 PDA 等移动设备病毒已出现，还将有更大的发展。

5. 攻击对象趋于混合型

随着防病毒技术的日新月异、传统软件保护技术的广泛探讨和应用，当今的计算机病毒在实现技术上有了一些质的变化，病毒攻击对象趋于混合，逐步转向对可执行文件和系统引导区同时感染，在病毒源码的编制、反跟踪调试、程序加密、隐蔽性、攻击能力等方面的设计都呈现了许多不同一般的变化。

6. 使用反跟踪技术

当用户或防病毒技术人员发现一种病毒时，一般都要先借助于 DEBUG 等调试工具对其进行详细分析、跟踪解剖。为了对抗动态跟踪，目前的病毒程序中一般都嵌入了一些破坏单步中断 INT 1H 和断点设置中断 INT 3H 的中断向量程序段，从而使动态跟踪难以完成。有的病毒则通过对键盘进行封锁，以禁止单步跟踪。

病毒代码还通过在程序中使用大量非正常的转移指令，使跟踪者不断迷路，造成分析困难。一般而言，CALL/RET、CALL FAR/RET、INT/IRET 命令都是成对出现的，返回地址的处理是自动进行的，不需编程者考虑，但是近来一些新的病毒肆意篡改返回地址，或者在程序中将上述命令单独使用，从而使用户无法迅速摸清程序的转向。

7. 增强隐蔽性

病毒通过各种手段，尽量避免出现容易使用户产生怀疑的病毒感染特征。

（1）避开修改中断向量值。许多防病毒软件都对系统的中断向量表进行监测，一旦发现任何有对系统内存中断向量表进行修改的操作，将首先认为有病毒在活动。因此，为避免修改中断向量表而留下痕迹，有些病毒直接修改中断服务子程序，取得对系统的控制权。病毒采用修改.com 文件首指针的方式修改中断服务子程序；首先从中断向量表中动态获得

中断服务子程序入口，然后将该入口开始处 3～5 字节内的指令内容保存到病毒体工作区，最后修改入口处指令，使其转向相应的病毒中断服务子程序入口，在执行修改后的子程序后，再由病毒控制转向原正常的服务子程序入口。例如，DIRII 病毒对 INT 21H 中断向量的控制就采用了类似的手法。

（2）请求在内存中的合法身份。病毒为躲避侦察常采用以下方法获得合法内存：通过正常的内存申请进行合法驻留，例如 DONG 病毒采用向内存高端申请 2000 字节的正常空间移入病毒体；通过修改内存控制链进驻内存；驻留低端内存，例如 DIRII 病毒驻留在用户可用内存空间的低端。所以，单从内存的使用情况上很难区分正常程序和病毒程序。

（3）维持宿主程序的外部特性。病毒截取 INT 21H 中断，控制原文件的显示，使已经被感染的程序在显示时不改变原来特征，例如长度、修改日期等。病毒也可能截取 INT 13H 中断，当发现有读硬盘主引导区或 DOS 分区的操作时，将用原来的正确内容显示给用户，以迷惑用户。

（4）不使用明显的感染标志。病毒不再简单地根据某个标志判断其本身是否已经在目标系统中存在，而是经过一系列相关运算来判断某个文件是否已被感染。

8．进行加密技术处理

（1）对程序段进行动态加密。病毒采取一边执行一边译码的方法，即后边的机器码是与前边的某段机器码运算后还原的，而用 DEBUG 等调试工具把病毒从头到尾打印出来，打印出的程序语句将是被加密的，无法阅读。

（2）对显示信息进行加密。例如，“新世纪”病毒在发作时，将显示一页书信，但作者对此段信息进行加密，从而不可能通过直接调用病毒体的内存映像寻找到它的踪影。

（3）对宿主程序段进行加密。病毒将宿主程序入口处的几个字节经过加密处理后存储在病毒体内，这给杀毒修复工作带来很大困难。

9．病毒不断繁衍不同变种

目前病毒已经具有许多智能化的特性，例如自我变形、自我保护、自我恢复等。在不同宿主程序中的病毒代码，不仅绝大部分不相同，且变化的代码段的相对空间排列位置也有变化。病毒能自动化整为零，分散潜伏到各种宿主中。对不同的感染目标，分散潜伏的宿主也不一定相同，在活动时又能自动组合成一个完整的病毒。例如，经过多态病毒感染的文件在不同的感染文件之间相似性极少，使得防病毒检测成为一项艰难的任务。

小　　结

计算机病毒防治是信息系统安全的一个重要方面，了解病毒的发展历史、病毒特点、分类等基本知识，理解病毒的作用机理，掌握基本的病毒检查、清除方法和防治管理措施，对于构建安全的信息系统、减小病毒所造成的损失具有积极的作用。

计算机病毒是指编制或在计算机程序中插入的破坏计算机功能或者破坏数据，影响计

算机使用并且能够自我复制的一组计算机指令或程序代码。它具有发生侵害的主动性、传染性、隐蔽性、表现性、破坏性、难确定性等特点。它们在结构上有着共同性，一般由引导模块、传染模块、表现模块 3 部分组成。

计算机病毒能够感染的只有可执行代码，按照可执行代码的种类可以将计算机病毒分为引导型病毒、文件型病毒、宏病毒和网络病毒四大类。各类病毒的工作机理不尽相同。了解计算机病毒工作机理对于防范计算机病毒、查杀计算机病毒和恢复染毒后的系统有着积极的意义。

恶意代码可以分成需要宿主的程序和可以独立运行的程序两类，其中包含了后门、逻辑炸弹、特洛伊木马、病毒和蠕虫等。

木马通常包含控制端和被控制端两部分，具有隐蔽性和非授权性的特点。它是一种远程控制工具，以简便、易行、有效而深受黑客青睐。木马病毒主要以网络为依托进行传播，窃取用户隐私资料是其主要目的。而且这些木马病毒多具有引诱性与欺骗性，是病毒新的危害趋势。可以通过查看系统端口开放的情况、系统服务情况、系统任务运行情况、网卡的工作情况、系统日志及运行速度有无异常等对木马进行检测。检测到计算机感染木马后，就要根据木马的特征来进行清除。最好的情况是不出现木马，这就要求我们平时要有对木马的预防意识和措施，做到防患于未然。

蠕虫的基本程序结构包含传播模块、隐藏模块和目的功能模块。其传播过程一般包括扫描、攻击和复制 3 个阶段。它具有传播迅速、难以清除、利用操作系统和应用程序的漏洞主动进行攻击、传播方式多样、病毒制作技术与传统的病毒不同、与黑客技术相结合等特点。对于企业用户来说，蠕虫病毒形成的威胁主要集中在服务器和大型应用软件上；而对个人用户，主要是要防范电子邮件和恶意网页传播方式与社会工程学结合所形成的威胁。

计算机病毒的防治是一个综合治理的社会问题，只有完善的规章制度和健全的管理体制，才能使措施到位，防患于未然，减少病毒入侵后所造成的损失。

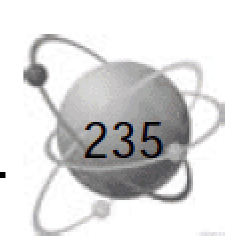
病毒预防是指根据系统特性，采取相应的系统安全措施预防病毒入侵计算机系统。

病毒检测就是要在特定的系统环境中，通过各种检测手段来识别病毒，并对可疑的异常情况进行报警。病毒检测主要是通过病毒扫描、系统完整性检查、分析法、校验和法和行为封锁法等 5 种手段进行。

较为流行的防病毒软件包括卡巴斯基、诺顿、NOD32 等国际品牌和江民 KV 系列、金山毒霸、瑞星杀毒软件、熊猫卫士等国产品牌。

计算机网络病毒实际上是一个笼统的概念。一种情况是，计算机网络病毒专指在网络上传播并对网络进行破坏的病毒；另一种情况是，计算机网络病毒指的是 HTML 病毒、E-mail 病毒、Java 病毒等与 Internet 有关的病毒。它除了具有可传播性、可执行性、破坏性、可触发性等计算机病毒的共性外，还具有感染速度快、扩散面广、传播的形式复杂多样、难以彻底清除和破坏性大等新特点。网络病毒查杀的重点应放在注册表和系统程序的维护上。

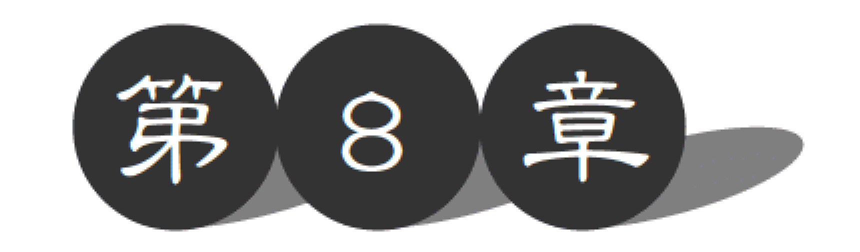
宏病毒由于易于理解、易于编写和修改，形成了变种多、传播广的特点，也为查杀病毒带来一定的难度。了解宏病毒的特征，正确维护宏病毒赖以生存的系统平台，可积极有效地防范宏病毒。



根据病毒的发展演变，可预见未来计算机病毒的更新换代将向多元化方向发展，可能具有病毒的网络化、病毒功能的综合化、传播途径的多样化、病毒的多平台化、攻击对象趋于混合型、使用反跟踪技术、增强隐蔽性、进行加密技术处理和不断繁衍不同变种等发展趋势。

练习与思考

1. 什么是计算机病毒？它有什么特点？它对系统的破坏主要表现为哪些形式？
2. 简述计算机病毒的发展史。
3. 常见的计算机病毒如何分类？每一类分类方法又可以分为哪几种？
4. 计算机病毒能够形成哪些危害？
5. 计算机病毒一般由哪些模块组成？每个模块的作用各是什么？
6. 各类计算机病毒的工作机理各是什么？
7. 什么是恶意代码？它可以分成哪两类？每一类分别包含了哪些恶意代码？试简述每一种恶意代码的特点。
8. 什么是木马？简述其工作原理和工作过程。
9. 木马具有哪些特点？它是如何进行传播的？简述其危害。
10. 如何检测和清除木马？如何预防木马？
11. 什么是蠕虫？它和普通病毒相比，有哪些异同？
12. 蠕虫的基本程序结构包含哪些模块？这些模块各自的功能分别是什么？
13. 简述蠕虫程序的传播过程。
14. 蠕虫病毒能够对网络形成哪些破坏？
15. 蠕虫病毒具有哪些特点？
16. 企业用户和个人用户分别应如何防范蠕虫病毒所形成的威胁？
17. 病毒进入系统，主要通过哪些途径进行传播？
18. 病毒预防可以采取哪些简单有效的措施？
19. 病毒检测可以采取哪些手段？简述每种手段的工作原理。
20. 当系统感染病毒以后，可以采取哪些措施进行紧急处理以恢复系统或受损部分？
21. 较为流行的防病毒软件包括哪些国际品牌和哪些国产品牌？
22. 简述瑞星杀毒软件的安装、菜单功能、使用和升级方法。
23. 网络病毒是如何进行传播的？它有哪些特点？
24. 网络病毒的防治工作具有哪些特点？
25. 举例说明如何检测与清除网络病毒。
26. 如何检测宏病毒的存在？如何防范和清除 Word 宏病毒？
27. 手机病毒与传统计算机病毒的区别在哪里？
28. 简述未来计算机病毒的发展趋势。



入侵检测系统

本章学习要求：

（1）掌握入侵检测技术的原理、类型、检测过程及其发展趋势。
（2）掌握网络扫描技术的类型和扫描过程。
（3）理解网络监听技术和网络嗅探器。
（4）了解几种商用入侵检测系统的特点及其工作机制。
（5）了解 IDS 的发展趋势及研究方向。

重点和难点：

（1）重点：入侵检测技术的原理和入侵检测系统的工作机制。
（2）难点：网络监听技术和网络嗅探器。

任何网络数据库系统都面临着各种网络安全的威胁，黑客、攻击者等网络入侵者利用网络系统的安全防护漏洞，大肆入侵系统获取机密，或对系统进行恶意破坏等。因此，快速的网络入侵检测和恢复对网络安全而言至关重要。

本章简单介绍入侵检测技术、网络扫描技术、网络监听技术和入侵检测系统方面的内容。

8.1　入侵检测的结构与原理

网络入侵检测是指从计算机网络的若干关键点收集信息并对其进行分析，从中查找网络中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定的软件与硬件的组合措施予以防治。

网络入侵检测技术是网络动态安全的核心技术，相关设备和系统是整个安全防护体系的重要组成部分。目前，防火墙沿用的仍是静态安全防御技术，对于网络环境下日新月异的攻击手段缺乏主动的响应，不能提供足够的安全保护；而网络入侵检测系统却能对网络



入侵事件和过程作出实时响应，与防火墙共同成为网络安全的核心设备。

8.1.1 入侵检测发展历史

自从计算机问世以来，安全问题就一直存在。特别是随着 Internet 的迅速扩张和电子商务的兴起，人们发现保护资源和数据的安全，使之免受来自恶意入侵者的威胁是件相当困难的事。提到网络安全，很多人首先想到的便是防火墙。防火墙作为一种静态的访问控制类安全产品，通常使用包过滤的技术来实现网络的隔离。适当配置的防火墙虽然可以将非预期的访问请求屏蔽在外，但不能检查出经过它的合法流量中是否包含着恶意的入侵代码。在这种需求背景下，入侵检测系统（Intrusion Detection System，IDS）应运而生。

入侵检测系统是将电子数据处理、安全审计、模式匹配及统计技术等有机地融合在一起，通过分析被检测系统的审计数据或直接从网络中捕获数据，查找其中是否有违背安全策略或危及系统安全的行为和活动。

入侵检测是一门综合性技术，既包括实时检测技术，也有事后分析技术。尽管用户希望通过部署 IDS 来增强网络安全，但不同的用户需求也不同，加之攻击的不确定性，单一的 IDS 产品可能无法做到面面俱到。因此，IDS 的未来发展必然是多元化的，只有通过不断改进和完善才能更好地协助网络进行安全防御。

入侵检测技术的发展已经历了 4 个主要阶段：

第一阶段是以协议解码和模式匹配为主的技术，其优点是对于已知的攻击行为非常有效，各种已知的攻击行为可以对号入座，误报率低；缺点是高超的黑客采用变形手法或者新技术可以轻易躲避检测，漏报率高。

第二阶段是以模式匹配+简单协议分析+异常统计为主的技术，其优点是能够分析处理一部分协议，可以进行重组；缺点是匹配效率较低，管理功能较弱。这种检测技术实际上是在第一阶段技术的基础上增加了部分对异常行为分析的功能。

第三阶段是以完全协议分析+模式匹配+异常统计为主的技术，其优点是误报率、漏报率和滥报率较低，效率高，可管理性强，并在此基础上实现了多级分布式的检测管理；缺点是可视化程度不够，防范及管理功能较弱。

第四阶段是以安全管理+协议分析+模式匹配+异常统计为主的技术，其优点是入侵管理和多项技术协同工作，建立全局的主动保障体系，具有良好的可视化、可控性和可管理性。以该技术为核心，可构造一个积极的动态防御体系，即入侵管理系统 IMS。

新一代的入侵检测系统应该是集成基于主机的入侵检测系统（Host-based Intrusion Detection System，HIDS）和基于网络的入侵检测系统（Network-based Intrusion Detection System，NIDS）的优点、部署方便、应用灵活、功能强大、并提供攻击签名、检测、报告和事件关联等配套服务功能的智能化系统。

目前的 IDS 还存在着很多缺陷：首先，目前的技术还不能对付训练有素的黑客的复杂攻击，其次，系统的虚警率太高；最后，系统需要对大量的数据进行处理，非但无助于解决问题，还降低了处理能力。

无论从规模还是从方法上，入侵技术近年来都发生了许多变化，入侵的手段与技术也有了“进步与发展”。入侵技术的发展与演化，主要反映在下列几个方面。

（1）入侵或攻击的综合化与复杂化。以前的入侵者往往采取一种攻击手段，随着网络防范技术的多重化，攻击的难度增加，如今入侵者在实施入侵或攻击时往往同时采取多种入侵的手段，以保证入侵的成功几率，并可在攻击实施的初期掩盖攻击或入侵的真实目的。

（2）入侵主体对象的间接化，即实施入侵与攻击的主体的隐蔽化。通过一定的技术，可掩盖攻击主体的源地址及主机位置，即使用了隐蔽技术后，对被攻击对象实施攻击的主体是无法直接确定的。

（3）入侵或攻击的规模扩大。对于网络的入侵与攻击，在其初期往往是针对于某公司或某个网站，其攻击的目的可能仅仅是为了炫耀技术能力、猎奇，当然也不排除商业的盗窃与破坏行为。由于战争对电子技术与网络技术的依赖性越来越大，随之产生、发展、逐步升级到电子战与信息战。对于信息战，无论其规模与技术都与一般意义上的计算机网络的入侵与攻击不可相提并论。信息战的成败与国家主干通信网络的安全，是与任何主权国家领土安全一样的国家安全。

（4）入侵或攻击技术的分布化。以往常见的入侵与攻击行为往往由单机执行，由于防范技术的发展使得此类行为往往不能奏效。于是，黑客们转而采用分布式攻击手段，如分布式拒绝服务 DDoS，在很短时间内即可造成被攻击主机的瘫痪，且此类分布式攻击的单机信息模式与正常通信无异，所以往往在攻击发动的初期不易被确认。分布式攻击是近期黑客最常用的攻击手段。

（5）攻击对象的转移。入侵与攻击常以网络为侵犯的主体，但近期来的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统，且有愈演愈烈的趋势。目前已有专门针对 IDS 进行攻击的报道。攻击者详细地分析了 IDS 的审计方式、特征描述、通信模式，从而找出 IDS 的弱点，然后加以攻击。

随着时代的发展，入侵检测技术将朝着 3 个方向发展。

（1）分布式入侵检测：第一层含义，即针对分布式网络攻击的检测方法；第二层含义，即使用分布式的方法来检测分布式的攻击，其中的关键技术为检测信息的协同处理与入侵攻击的全局信息的提取。

（2）智能化入侵检测：即使用智能化的方法与手段来进行入侵检测。所谓的智能化方法，现阶段常用的有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一。特别是具有自学能力的专家系统，实现了知识库的不断更新与扩展，设计的入侵检测系统的防范能力不断增强，具有更广泛的应用前景。应用智能化的概念来进行入侵检测的尝试也已有报道。较为一致的解决方案应为高效常规意义下的入侵检测系统与具有智能检测功能的检测软件或模块的结合使用。

（3）全面的安全防御方案：即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位对所关注的网络作出全面的评估，然后提出可行的整体解决方案。

8.1.2　入侵检测原理与系统结构

1. 入侵检测原理

入侵检测可分为实时入侵检测和事后入侵检测，其原理分别如图 8-1 和图 8-2 所示。

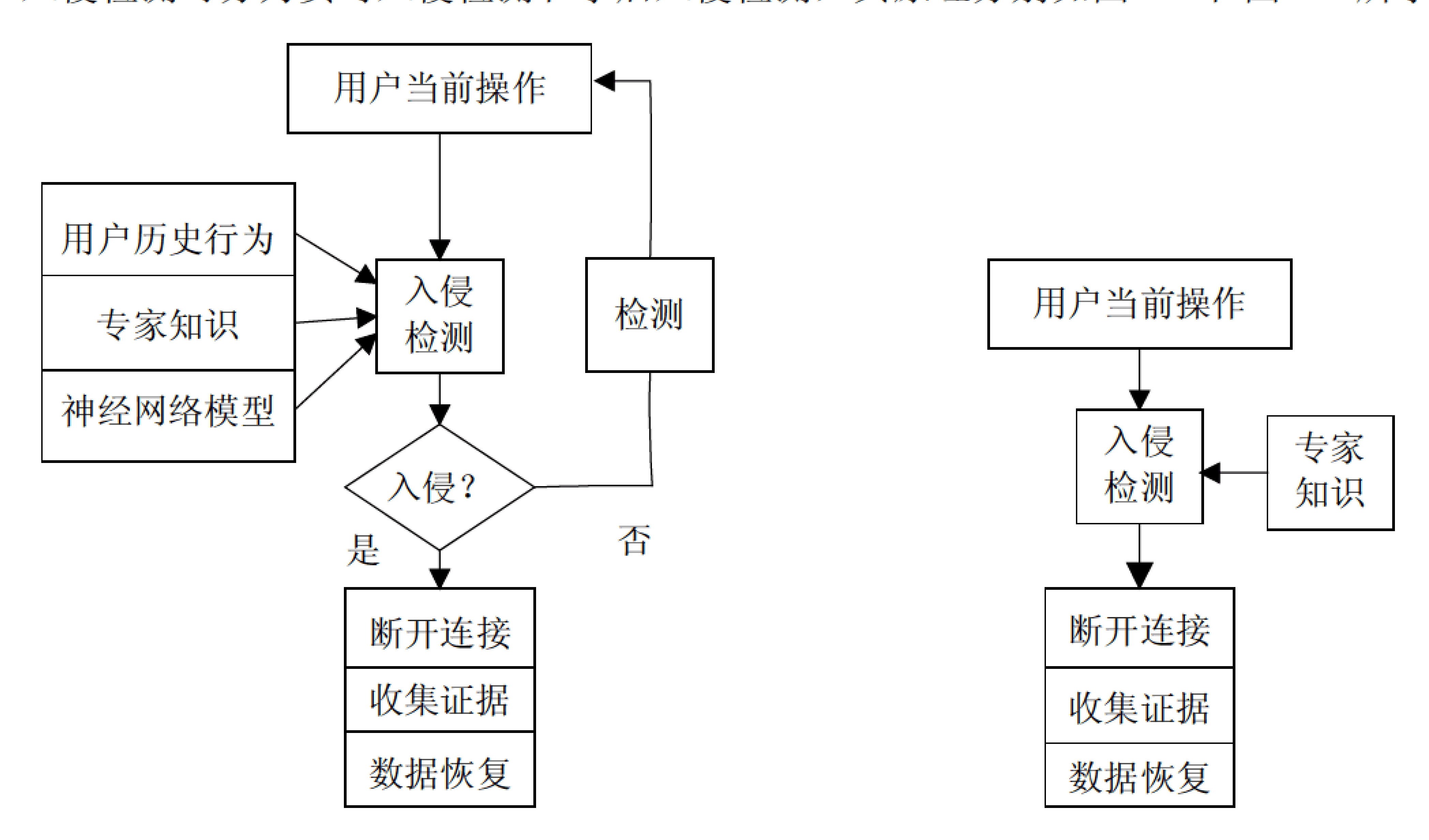


图 8-1　实时入侵检测原理　　　图 8-2　事后入侵检测原理

实时入侵检测在网络连接过程中进行，系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断，一旦发现入侵迹象立即断开入侵者与主机的连接，并收集证据和实施数据恢复。事后入侵检测由网络管理人员定期或不定期进行，根据计算机系统对用户操作所做的历史审计记录判断用户是否具有入侵行为，如果有就断开连接，并记录入侵证据和进行数据恢复；但是其入侵检测的能力不如实时入侵检测系统。

2. 入侵检测的过程

所谓入侵检测，就是从计算机网络或计算机系统中若干关键点收集信息并对其进行分析，从中查找网络或系统中是否有违反安全策略的行为和遭到攻击的迹象，同时作出响应。

入侵检测通过执行以下任务来实现：

- 监视、分析用户及系统活动。
- 系统构造和弱点的审计。
- 识别反映已知进攻的活动模式并向相关人士报警。
- 异常行为模式的统计分析。
- 评估重要系统和数据文件的完整性。
- 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

入侵检测的一般过程包括信息收集和信息检测分析。



（1）信息收集

网络入侵检测的第一步是信息收集，内容包括系统、计算机网络、数据及用户活动的状态和行为。而且，需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息。这除了尽可能扩大检测范围的因素外，还有一个重要的因素就是从一个信息源来的信息有可能看不出疑点，但从几个源来的信息的不一致性却是可疑行为或入侵的最好标识。入侵检测很大程度上依赖于收集信息的可靠性和正确性。入侵检测利用的信息一般来自以下 4 个方面：

① 系统和计算机网络日志文件

入侵者经常在系统日志文件中留下他们的踪迹，因此充分利用系统和计算机网络日志文件信息是检测入侵的必要条件。日志文件中记录了各种行为类型，每种类型又包含不同的信息，例如记录“用户活动”类型的日志就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。

② 目录和文件中不期望的改变

计算机网络环境中的文件系统包含很多软件和数据文件，其中含有重要信息的文件和私有数据文件经常是攻击者修改或破坏的目标。目录和文件中不期望的改变（包括修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。攻击者经常替换、修改和破坏他们获得访问权的系统中的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

③ 程序执行中的不期望行为

计算机网络系统中的程序一般包括操作系统、计算机网络服务、用户启动的程序和特定目的的应用。每个在系统上执行的程序由一到多个进程实现，而每个进程又在具有不同权限的环境中执行，这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现，操作执行的方式不同，它利用的系统资源也就不同。

一个进程出现了不期望的行为，表明可能有人正在入侵该系统。入侵者可能会将程序或服务的运行分解，从而导致它失败，或者是以非用户或管理员意图的方式操作。

④ 物理形式的入侵信息

这包括两个方面的内容，一是未授权的对计算机网络硬件的连接；二是对物理资源的未授权访问。入侵者会想方设法去突破计算机网络的周边防卫，如果他们能够在物理上访问内部网，就能安装他们自己的设备和软件，进而探知网上由用户加上去的不安全（未授权）设备，然后利用这些设备访问计算机网络。

（2）信息检测分析

信息收集器将收集到的有关系统、计算机网络、数据及用户活动的状态和行为等信息传送到分析器，由分析器对其进行分析。分析器一般采用 3 种技术对其进行分析：模式匹配、统计分析和完整性分析。前两种方法用于实时的计算机网络入侵检测，而完整性分析用于事后的计算机网络入侵检测。

① 模式匹配

模式匹配就是将收集到的信息与已知的计算机网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单（例如通过字符串匹配以寻找一个简单的条目或指令），也可以很复杂（例如利用正规的数学表达式来表示安全状态的变化）。该方法的一大优点是只需收集相关的数据集合，显著减轻了系统负担，且技术已相当成熟；与病毒防火墙采用的方法一样，检测的准确率和效率都相当高。但是，该方法的弱点就是需要不断地升级以对付不断出现的攻击手段，不能检测到从未出现过的攻击手段。

② 统计分析

统计分析方法首先给系统对象（例如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（例如访问次数、操作失败次数和时延等）。测量属性的平均值将被用来与计算机网络、系统的行为进行比较，任何观察值在正常范围之外时，就认为有入侵发生。其优点是可检测到未知的入侵和更为复杂的入侵；缺点是误报、漏报率高，且不适应用户正常行为的突然改变。具体的统计分析方法有基于专家系统的分析方法、基于模型推理的分析方法和基于神经计算机网络的分析方法。

③ 完整性分析

完整性分析主要关注某个文件或对象是否被更改。完整性分析利用强有力的加密机制（称为消息摘要函数），能够识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能发现。缺点是一般以批处理方式实现，不用于实时响应。尽管如此，完整性检测方法依然是维护计算机网络安全的必要手段之一。例如，可以在每一天的某个特定时间内开启完整性分析模块，对计算机网络系统进行全面的扫描检查。

3. 入侵检测系统的模型

根据入侵检测的原理，入侵检测系统至少应该包含 3 个模块，即提供信息的信息源、发现入侵迹象的分析器和入侵响应部件。为此，美国国防部高级计划局提出了公共入侵检测模型（Common Intrusion Detection Framework，CIDF），阐述了一个入侵检测系统 IDS 的通用模型。它将一个入侵检测系统分为 4 个组件，如图 8-3 所示。

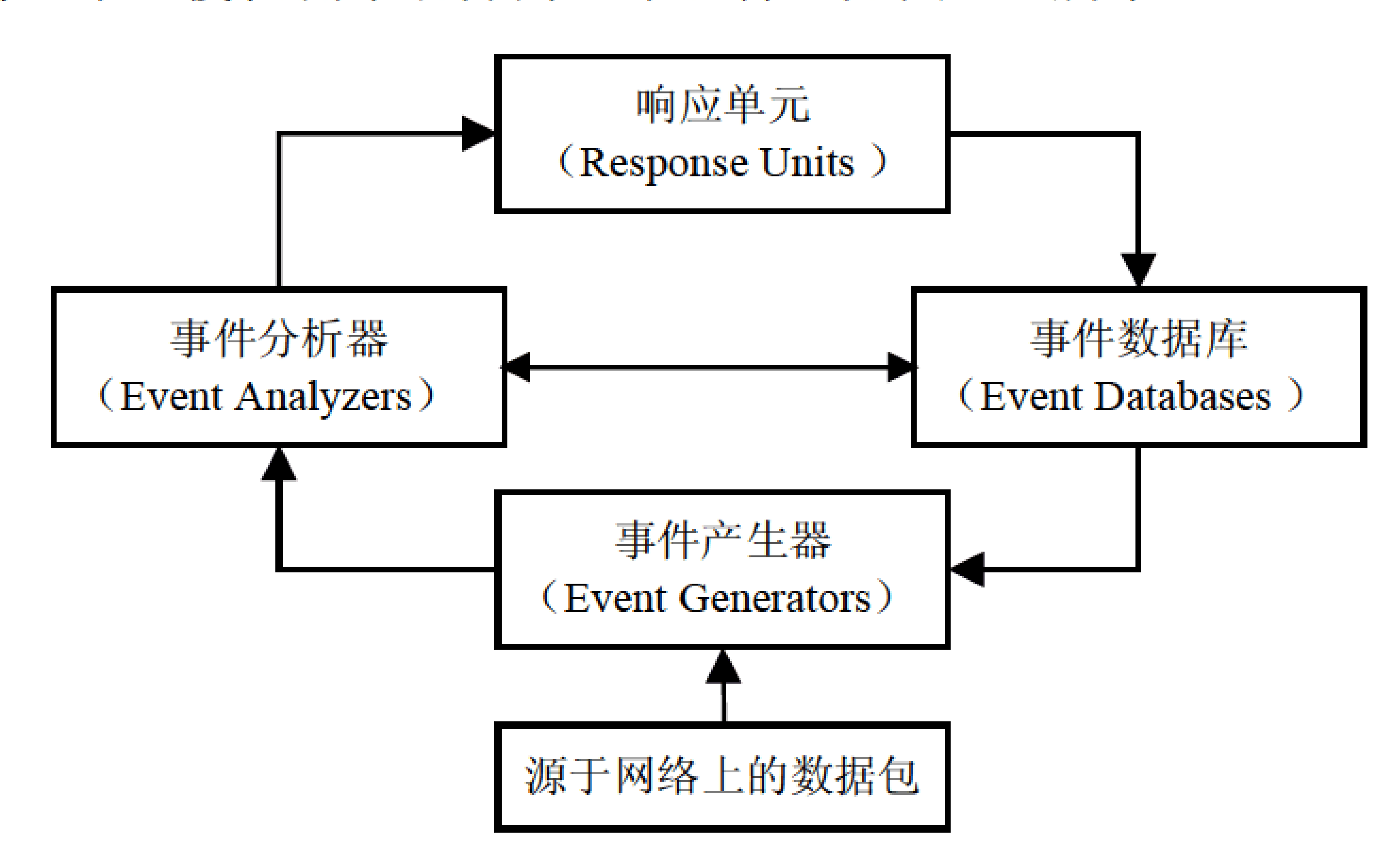


图 8-3　入侵检测系统的组成

（1）事件产生器

事件产生器从系统所处的计算机网络环境中收集事件，并将这些事件转换成一定格式以传送给其他组件。可以说，事件产生器是实时监视网络数据流并依据入侵检测规则产生事件的一种过滤器。

（2）事件数据库

事件数据库用来存储事件产生器和事件分析器产生的临时事件，以备系统需要的时候使用。事件数据库保存的事件信息，包括正常事件信息和入侵事件信息，也包括存储的临时处理数据，扮演各个组件之间的数据交换中心。

（3）事件分析器

事件分析器可以是一个特征检测工具，用于在一个事件序列中检查是否有已知的攻击特征；也可以是一个统计分析工具，检查现在的事件是否与以前某个事件来自同一个事件序列；此外，事件分析器还可以是一个相关器，观察事件之间的关系，将有联系的事件放到一起，以利于以后的进一步分析。

（4）响应单元

响应单元根据事件产生器检测到的和事件分析器分析到的入侵行为而采取相应的响应措施。在检测到入侵攻击后，基于网络的入侵检测系统的响应单元主要有两类响应方式：被动响应方式和主动响应方式。被动响应方式是系统在检测出入侵攻击后只是产生报警和日志通知管理员，具体处理工作由管理员完成；主动响应方式是系统在检测出入侵攻击后，可以自动对目标系统或者相应网络设备作出修改制止入侵行为。

在网络入侵检测系统模型中，事件产生器、事件分析器和响应单元通常以应用程序的形式出现，而事件数据库则往往以文件或数据流的形式出现。这 4 个组件是网络入侵检测系统最核心的部分，可以完成最基本的入侵检测功能。但是作为一个完整的网络入侵检测系统，系统管理组件和日志审计组件也是必不可少的。系统管理组件完成对系统的操作与配置，而日志审计组件是任何安全设备必须具备的功能。系统管理组件负责网络入侵检测系统的管理，主要包括权限管理、设备管理、规则管理、升级管理；日志审计组件完成对操作日志和入侵检测日志的审计。

8.1.3 入侵检测系统的分类

1. 根据检测原理分类

根据检测原理的属性可以将入侵分为异常和滥用两种，两者分别建立了相应的异常检测模型和滥用检测模型。

（1）异常检测模型：检测与可接受行为之间的偏差。如果可以定义每项可接受的行为，那么每项不可接受的行为就应该是入侵。首先总结正常操作应该具有的特征，当用户活动与正常行为有重大偏离时即被认为是入侵。这种检测模型因为不需要对每种入侵行为进行定义，所以能有效检测未知的入侵，即漏报率低，但误报率高。

（2）滥用检测模型：检测与已知的不可接受行为之间的匹配程度。如果可以定义所有



的不可接受行为，那么每种能够与之匹配的行为都会引起报警。收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。这种检测模型误报率低、漏报率高。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击却效果有限，而且特征库必须不断更新。

2．按照检测对象划分

（1）基于主机的入侵检测系统 HIDS：系统分析的数据是计算机操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录。主机型入侵检测系统保护的一般是所在的主机系统，是由代理来实现的。代理是运行在目标主机上的小的可执行程序，它们与命令控制台通信。

（2）基于网络的入侵检测系统 NIDS：系统分析的数据是网络上的数据包。基于网络的入侵检测系统由遍及网络的传感器组成，担负着保护整个网段的任务。传感器是一台将以太网卡置于混杂模式的计算机，用于嗅探网络上的数据包。

（3）混合型的入侵检测系统：基于主机和基于网络的入侵检测系统都有不足之处，会造成防御体系的不全面；而综合了两者优点的混合型入侵检测系统既可以发现网络中的攻击信息，也可以从系统日志中发现异常情况。

3．根据体系结构分类

根据体系结构，可以将入侵检测系统（IDS）分为集中式、等级式和协作式 3 种。

（1）集中式入侵检测系统有一个中央入侵检测服务器和多个分布在不同主机上的审计程序。审计程序将收集的数据发送给中央服务器进行处理和分析。这种体系结构对中央服务器的数据处理能力和安全性都提出了极高的要求。

（2）等级式入侵检测系统定义了若干个分等级的监控区，每一级监控区负责自己本层的数据分析并提交到上一级监控区。它将分析处理难度分摊，但是安全性没有得到提高，而且对网络拓扑结构的依赖性也比较大。

（3）协作式入侵检测系统综合了前两者的优点，扬长避短。各个 IDS 不分等级，相互协同工作，效率很高；但是设计难度大，维护成本也很高。

4．从技术方面分类

从技术上讲，入侵检测技术可以大致分为基于知识的模式识别、基于知识的异常识别和协议分析 3 类；而主要的入侵检测方法有特征检测法、概率统计分析法和专家知识库系统。

（1）基于知识的模式识别

这种技术是通过事先定义好的模式数据库实现的。其基本思想是：首先把各种可能的入侵活动均用某种模式表示出来，并建立模式数据库，然后监视主体的一举一动，当检测到主体活动违反了事先定义的模式规则时，根据模式匹配原则判别是否发生了攻击行为。

这种模式识别的关键是建立入侵模式的表示形式，同时要能够区分入侵行为和正常行为。这种检测技术仅限于检测出已建立模式的入侵行为，对新型的入侵是无能为力的，仍

需改进。

（2）基于知识的异常识别

这种技术是通过事先建立正常行为档案库实现的。其基本思想是：首先把主体的各种正常活动用某种形式描述出来，并建立“正常活动档案”，当某种活动与所描述的正常活动存在差异时，就认为是“入侵”行为，进而被检测识别。利用行为进行识别时存在四种可能：一是入侵且行为正常；二是入侵且行为异常；三是非入侵且行为正常；四是非入侵且行为异常。根据异常识别思想，把第二种和第四种情况判定为“入侵”行为。这种检测技术可以检测出未知行为，并具有简单的学习功能。以下是几种基于知识的异常识别检测方法：

① 基于审计的攻击检测技术

这种检测方法是通过对审计信息的综合分析实现的。其基本思想是：根据用户的历史行为、先前的证据或模型，使用统计分析方法对用户当前的行为进行检测和判别，当发现可疑行为时，保持跟踪并监视其行为，同时向系统安全员提交安全审计报告。

② 基于神经网络的攻击检测技术

由于用户的行为十分复杂，要准确匹配一个用户的历史行为和当前行为是相当困难的，这也是基于审计攻击检测的主要弱点。基于神经网络的攻击检测技术代表了基于传统统计技术的攻击检测方法的改进方向，它能够解决传统的统计分析技术所面临的若干问题，例如建立确切的统计分布、实现方法的普遍性、降低算法实现的成本和系统优化等问题。

③ 基于专家系统的攻击检测技术

所谓专家系统就是一个依据专家经验定义的推理系统。这种检测是建立在专家经验基础上的，它根据专家经验进行推理判断得出结论。例如，当用户连续 3 次登录失败时，可以把该用户的第四次登录视为攻击行为。

④ 基于模型推理的攻击检测技术

攻击者在入侵一个系统时往往采用一定的行为程序（如猜测口令的程序），这种行为程序构成了某种具有一定行为特征的模型，根据这种模型所代表的攻击意图的行为特征，可以实时地检测出恶意的攻击企图，尽管攻击者不一定都是恶意的。用基于模型的推理方法，人们能够为某些行为建立特定的模型，从而能够监视具有特定行为特征的某些活动。根据假设的攻击脚本，这种系统就能检测出非法的用户行为。一般为了准确判断，要为不同的入侵者和不同的系统建立特定的攻击脚本。

使用基于知识的模式识别和基于知识的异常识别所得出的结论差异较大，甚至会得出相反的结论。这是因为基于知识的模式识别的核心是维护一个入侵模式库，它对已知攻击可以详细、准确地报告出攻击类型，但对未知攻击却无能为力，而且入侵模式库必须不断更新；而基于知识的异常识别则是通过对入侵活动的检测得出结论的，它虽无法准确判断出攻击的手段，但可以发现更广泛的、甚至未知的攻击行为。

（3）协议分析

这种检测方法是根据针对协议的攻击行为实现的。其基本思想是：首先把各种可能针对协议的攻击行为描述出来，然后建立用于分析的规则库，最后利用传感器检查协议中的

有效负荷，并详细解析，从而实现入侵检测。

8.1.4　入侵检测的主要性能指标

网络入侵检测系统的性能指标主要包括 3 项，即准确性指标、效率指标和系统指标。

1. 准确性指标

准确性指标在很大程度上取决于测试时采用的样本集和测试环境。样本集和测试环境不同，准确性也不相同。主要包括 3 个指标，即检测率、误报率和漏报率。

① 检测率是指被监视网络在受到入侵攻击时，系统能够正确报警的概率。通常利用已知入侵攻击的实验数据集合来测试系统的检测率。检测率=入侵报警的数量/入侵攻击的数量。

② 误报率是指系统把正常行为作为入侵攻击而进行报警的概率和把一种已知的攻击错误报告为另一种攻击的概率。误报率=错误报警数量/(总体正常行为样本数量+总体攻击样本数量)。

③ 漏报率是指被检测网络受到入侵攻击时，系统不能正确报警的概率。通常利用已知入侵攻击的实验数据集合来测试系统的漏报率。漏报率=不能报警的数量/入侵攻击的数量。

2. 效率指标

效率指标根据用户系统的实际需求，以保证检测质量为准；同时取决于不同的设备级别，例如百兆网络入侵检测系统和千兆网络入侵检测系统的效率指标一定有很大差别。效率指标主要包括最大处理能力、每秒并发 TCP 会话数、最大并发 TCP 会话数等。

① 最大处理能力是指网络入侵检测系统在检测率下系统没有漏报警的最大处理能力，目的是验证系统在检测率下能够正常报警的最大流量。

② 每秒并发 TCP 会话数是指网络入侵检测系统每秒最大可以增加的 TCP 连接数。

③ 最大并发 TCP 会话数是指网络入侵检测系统最大可以同时支持的 TCP 连接数。

3. 系统指标

系统指标主要表征系统本身运行的稳定性和使用的方便性。系统指标主要包括最大规则数、平均无故障间隔等。

① 最大规则数：系统允许配置的入侵检测规则条目的最大数目。

② 平均无故障间隔：系统无故障连续工作的时间。

由于网络入侵检测系统是软件与硬件的组合，故性能指标同样取决于软、硬件两方面的因素。软件因素主要包括数据重组效率、入侵分析算法、行为特征库等因素；硬件因素主要包括 CPU 处理能力、内存大小、网卡质量等因素。另外，由于网络安全的要求在提高，黑客攻击技术、漏洞发现技术和入侵检测技术在不断发展，网络入侵检测系统的升级管理功能也是重要的指标之一。用户应及时更新入侵特征库或升级软件版本，保证网络入侵检测系统的有效性。

8.1.5 入侵检测系统的部署

1. 入侵检测系统的发展

入侵检测系统（IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。与其他网络安全设备的不同之处在于，IDS 是一种积极主动的安全防护技术。IDS 最早出现在 1980 年 4 月，James P. Anderson 为美国空军作了一份题为《Computer Security Threat Monitoring and Surveillance》的技术报告，在其中他提出了 IDS 的概念。到了 20 世纪 80 年代中期，IDS 逐渐发展成为入侵检测专家系统 IDES。1990 年，IDS 分化为基于网络的 IDS 和基于主机的 IDS，随后又出现了分布式 IDS。

由于入侵检测系统的市场在近几年中飞速发展，许多公司开始投入到这一领域上来。除了国外的 ISS、Axent、NFR、Cisco 等公司外，国内也有数家公司（例如中联绿盟、中科网威等）推出了自己相应的产品。但就目前而言，入侵检测系统还缺乏相应的标准。目前，有两个组织试图对 IDS 进行标准化，即 IETF 的 IDWG（Intrusion Detection Working Group）和 CIDF（Common Intrusion Detection Framework），但进展非常缓慢，尚没有被广泛接受的标准出台。

目前，入侵检测产品的主要厂商有 ISS 公司（RealSecure）、Axent 公司（ITA、ESM），以及 NAI（CyberCop Monitor）。它们都在入侵检测技术上有着多年的研究。其中，ISS 公司的 RealSecured 智能攻击识别技术是当前 IDS 系统中最为先进的。

2. 入侵检测系统的作用

入侵检测系统作为一种积极主动的安全防护工具，提供了对内部攻击、外部攻击和误操作的实时防护，在计算机网络和系统受到危害之前进行报警、拦截和响应。其主要作用归纳如下：

（1）监视用户和系统的运行状况，查找非法用户和合法用户的越权操作。

（2）检测系统配置的正确性和安全漏洞，并提示管理人员修补漏洞。

（3）对用户的非正常活动进行统计分析，发现入侵行为的规律。

（4）检查系统程序和数据的一致性和正确性，例如计算和比较文件系统的校验和。

（5）能够实时对检测到的入侵行为进行反应。

（6）操作系统的审计跟踪管理。

入侵检测系统在网络安全和军事斗争中起到了非常重要的作用；而在经济领域中，它可以及时发现、阻拦入侵行为，保护企业来自不满员工、黑客和竞争对手的威胁，保证企业信息平台的正常运转……由此也决定了入侵检测系统商业化的必然趋势。

3. 入侵检测系统的部署

在目前的网络拓扑中，已经很难找到以前 Hub 式的共享介质冲突域的网络，绝大部分的网络区域都已经全面升级到交换式的网络结构。因此，IDS 在交换式网络中的位置一般

选择在尽可能靠近攻击源和受保护的资源处（通常是在服务器区域的交换机上、Internet 接入路由器之后的第一台交换机上或重点保护网段的局域网交换机上）。

经典入侵检测系统的部署方式如图 8-4 所示。

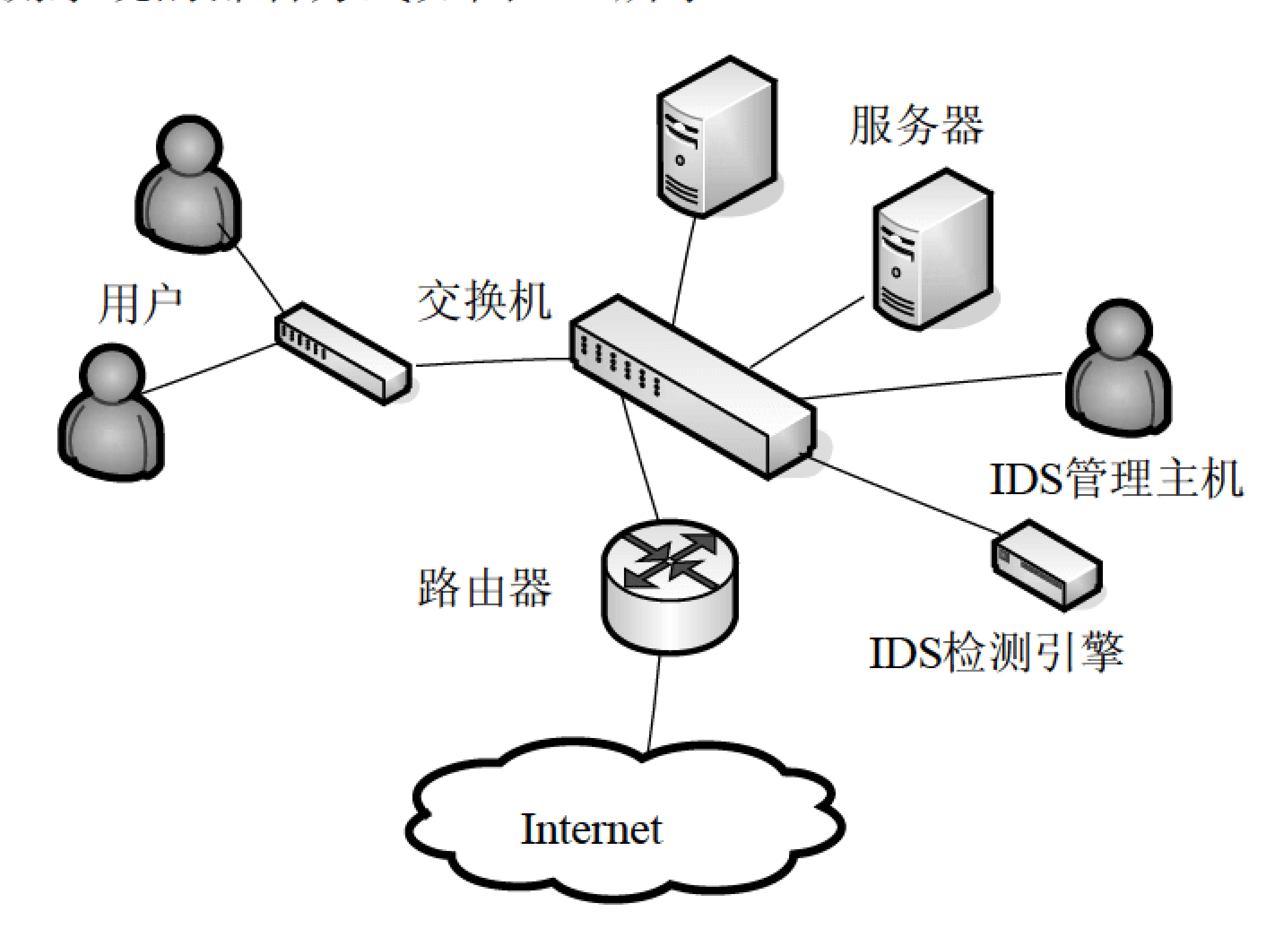


图 8-4　经典的入侵检测系统的部署方式

8.2　网络扫描和网络监听

8.2.1　网络系统的漏洞

1．网络系统漏洞的概念

网络系统漏洞也称为网络系统的脆弱性、缺陷等，是指网络系统的软件、硬件或策略上的不安全因素。网络系统漏洞可以分为两类：软漏洞和硬漏洞。软漏洞是由网络系统配置不当引起的；硬漏洞是软件或硬件厂商的生产过程造成的。网络系统的脆弱性是网络安全评估的测试对象，评估者对其的理解和测试方法是影响评估结果的决定因素。

2．网络系统漏洞的主要表现

网络系统的漏洞主要表现在以下几个方面：

1）网络操作系统的缺陷

（1）网络操作系统体系结构自身并不安全：操作系统程序具有动态连接性；操作系统可以在远程节点上创建并激活进程，被创建的进程还可以继续创建其他进程；网络操作系统为了维护的方便而预留的无口令入口成了黑客的通道。

（2）计算机系统的软件和硬件故障，例如硬盘故障、电源故障、芯片故障等造成了计算机系统的脆弱性。

（3）网络端口、传输线路和处理机有可能因屏蔽不严而造成电磁信息辐射，从而造成信息泄露。

2）软件安全漏洞

网络信息系统由硬件和软件组成。由于软件程序的复杂性和编程的多样性，在网络信息系统的软件中很容易有意或无意地留下一些不易被发现的安全漏洞。软件安全漏洞主要有以下几个方面：

（1）应用软件的安全漏洞

所谓应用软件的安全漏洞，是指应用软件在逻辑设计上的缺陷或在编写时产生的错误，该缺陷或错误可以被不法者或计算机黑客利用，通过植入木马、病毒等方式来攻击或控制整个计算机，从而窃取用户计算机中的重要资料和信息，甚至破坏用户的系统。

（2）操作系统的安全漏洞

操作系统是整个网络信息系统的核心控制软件，直接影响整个系统的信息安全。操作系统的安全漏洞主要有输入/输出的非法访问和操作系统陷门两大类。

① 输入/输出的非法访问

非法访问包括两种：一种是一些操作系统对输入/输出操作只检查一次，第一次检查通过后，往后的输入/输出操作就不再检查了，为后续的非法访问创造了条件；另一种是一些操作系统使用没有严格保护的公共系统缓冲区，任何用户都可以搜索这个缓冲区，其中的一些机密信息（口令、账号等）就可能被泄露。

② 操作系统陷门

某些操作系统为了安装其他公司的软件包而保留了一种特殊的管理程序功能，尽管此管理功能的调用需要以特权方式进行，但是并未受到严密的监控，缺乏必要的认证和访问权的限制，有可能被用于安全访问控制，从而形成操作系统陷门。

为了建立安全的操作系统，首先必须构造操作系统的安全模型和不同的实施方法；其次应该采用诸如隔离等安全、科学的操作系统设计方法；此外，还需要建立和完善操作系统的评估标准、评价方法和质量测试。

（3）数据库的安全漏洞

数据库管理系统 DBMS 作为管理数据库所有数据记录的应用软件系统，要求用户在访问数据时必须通过身份和权限验证，以保证系统自身的安全。但是，有些数据库将原始数据以明文的形式存储在数据库中，使得入侵者有机会从系统的后备存储器上窃取数据或篡改数据。因此，应对存储的数据进行加密保护，并且数据库的加密应该采取独特的加密和密钥管理方法。

（4）通信系统和通信协议的安全漏洞

网络的通信线路面对各种威胁时变得非常脆弱，非法用户对物理通信线路肆意进行破坏、搭线窃听，通过未保护的外部线路访问系统内部信息等。另外，通信网运行机制所基于的通信协议本身也存在一定的缺陷。

在网络信息系统中，通信协议作为一种规则，使得不了解的双方能够相互配合并保证公平性，据此建立、维护和解除通信联系，实现不同机型的互联。其基本特点是：预先建立、相互约定、无歧义、完备性。

高速信息网在技术上以传统电信网为基础，通过改革传输协议发展而来，因此各种传

输协议之间的不一致性也大大影响了信息的安全质量。例如互联网协议 TCP/IP，由于使用的广泛性，使得 TCP/IP 的任何安全漏洞都会产生巨大的影响。而 TCP/IP 提出之初，设计者将主要目标定位于“网络互联”，没有过多地考虑安全问题，例如它传输的信息采用明文方式。因此，TCP/IP 存在天生的缺陷。

（5）网络软件与网络服务的安全漏洞

比较常见的网络软件与网络服务的漏洞有：

① Finger 漏洞

在 TCP/IP 协议中，Finger 只需一个 IP 地址便可以提供许多关于主机的信息，例如谁正在登录、登录时间、登录地点等。对于一个训练有素的网络黑客来说，Finger 无疑是其入侵目标主机的一把利器。

② 匿名 FTP

匿名 FTP 即匿名文件传输协议。系统管理员建立了一个特殊的用户 ID，名为 anonymous，Internet 上的任何人在任何地方都可使用该用户 ID 登录远程计算机，将公共文件传输到用户的本地计算机。

③ 远程登录

在大型网络环境下，远程登录可以给用户带来很大方便，但在方便的背后却潜藏着很大的安全隐患。在网络上运行诸如 rlogin、rcprexec 等远程命令时，由于要跨越一些网络传输口令，而 TCP/IP 对所传输的信息又不进行加密，所以网络黑客只要在所攻击的目标主机的 IP 数据包所经过的一条路由上运行“嗅探器”（Sniffer）程序，就可以截取目标口令，给网络安全和信息保密带来很大威胁。

④ 电子邮件

内部网用户进行电子邮件发送和接收时存在被黑客跟踪或收到一些恶意程序（例如特洛伊木马、蠕虫等）、病毒程序等的可能，由于许多用户的安全意识比较淡薄，对一些来历不明的邮件警惕性不高，这就给了入侵者以可乘之机，直接威胁到系统安全。

⑤ 密码设置漏洞

服务系统登录和主机登录使用的是静态口令，口令在一定时间内是不变的，且在数据库中有存储记录，可重复使用。这样，非法用户通过网络窃听、非法数据库访问、穷举攻击、重放攻击等手段很容易得到这种静态口令，然后利用口令即可对资源进行非法访问和越权操作。

8.2.2　网络扫描

1．网络扫描技术

网络扫描技术是一种基于 Internet 远程检测目标网络或本地主机安全性脆弱点的技术。扫描采取模拟攻击的形式，对目标可能存在的已知安全漏洞逐项进行检查。目标可以是工作站、服务器、交换机、路由器和数据库应用等。通过扫描，系统管理员能够发现所维护的 Web 服务器的各种 TCP/IP 端口的分配、开放的服务、Web 服务的软件版本及软件呈现

在 Internet 上的安全漏洞，并根据扫描结果提供周密、可靠的分析报告。网络扫描技术与防火墙、安全监控系统互相配合就能够为网络提供很高的安全性。

2. 网络扫描的一般步骤

一次完整的网络安全扫描，分为如下 3 个阶段。

（1）第一阶段：发现目标主机或网络。

（2）第二阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务以及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

（3）第三阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

3. 网络扫描技术的分类

网络扫描技术主要包括 ping 扫描、端口扫描以及漏洞扫描等。其中端口扫描技术和漏洞扫描技术是网络安全扫描技术中的两种核心技术，并被广泛运用于当前较成熟的网络扫描器中，例如著名的 Nmap 和 Nessus。

（1）ping 扫描

ping 扫描用于网络安全扫描的第一阶段，可以判断出系统是否处于活动状态。ping 扫描有两种实现方式：

① ICMPping 扫描

该类扫描处于 TCP/IP 协议的网络层。其扫描过程：首先向被扫描的网络中的所有 IP 地址发送 ICMP-REQUEST 数据报，如果从某 IP 地址返回 ICMP-REPLAY 数据报，则表示该 IP 地址的主机在网络中存在并处于活动状态。

② TCP ping 扫描

该类扫描处于 TCP/IP 协议的传输层，主要利用 TCP 连接的 3 次握手特性和 TCP 数据头中的标志位来进行，也就是所谓的半开扫描。

（2）端口扫描技术

端口扫描用于网络安全扫描的第二阶段，通过与目标系统的 TCP/IP 端口连接，可以查看该系统是否处于监听或运行的状态。

一个端口就是一条潜在的通信通道，也就可能成为一条入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息，如系统目前向外界提供了哪些服务，存在哪些安全漏洞等，从而对症下药，有的放矢地予以防治。

端口扫描的原理是向目标主机的 TCP/IP 服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭的，就可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地主机或服务器的流入/流出 IP 数据包来监视本地主机的运行情况，不过它仅能对接收到的数据进行分析，帮助发现目标主机某些内在的弱点，而不会提供进入一个系统的详细步骤。端口扫描主要有经典的全连接扫描以及半连接扫描。此外，还有间接扫描和秘密扫描等。

① 全连接扫描

全连接扫描是 TCP 端口扫描的基础，现有的全连接扫描有 TCP connect 扫描和 TCP 反向 ident 扫描等。其中，TCP connect 扫描的实现原理如下所述：

扫描主机通过 TCP/IP 协议的 3 次握手与目标主机的指定端口建立一次完整的连接。连接由系统调用 connect 开始。如果端口开放，则连接建立成功；否则，返回-1，表示端口关闭。建立连接时，如响应扫描主机的 SYN/ACK 连接请求，则表明目标端口处于监听（打开）的状态；如果目标端口处于关闭状态，则目标主机会向扫描主机发送 RST 响应。

② 半连接扫描

若端口扫描没有完成一次完整的 TCP 连接，如在扫描主机和目标主机的一指定端口建立连接时只完成了前两次握手，在第三步时，扫描主机中断了本次连接，使连接没有完全建立起来，这样的端口扫描称为半连接扫描，也称为间接扫描。

（3）漏洞扫描

网络安全扫描的第三阶段采用的漏洞扫描通常是在端口扫描的基础上，对得到的信息进行相关处理，进而检测出目标系统存在的安全漏洞。

漏洞扫描主要通过下面的两种方法来检查目标主机是否存在漏洞：在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否有满足匹配条件的漏洞存在；通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，例如测试脆弱性口令等。若模拟攻击成功，则表明目标主机系统存在安全漏洞。

网络安全扫描技术是新兴的技术，与防火墙、入侵检测等技术相比，它是从另一个角度来解决网络安全上的问题。随着网络的发展和内核的进一步修改，新的端口扫描技术及对入侵性端口扫描的新防御技术还会不断诞生，到目前为止还没有一种完全成熟、高效的端口扫描防御技术；同时，漏洞扫描面向的漏洞包罗万象，而且漏洞的数目也在继续增加。就目前的漏洞扫描技术而言，自动化的漏洞扫描无法得以完全实现，而且新的难题也将不断涌现，因此网络安全扫描技术仍有待更进一步的研究和完善。

8.2.3 网络监听

1. 网络监听的概念

网络监听就是网络管理员利用一些工具软件监视网络的状态和数据流动情况，以便发现网络中的异常情况和不安全因素。

网络监听可以在网上任何一个位置进行，但是监听效果最好的地方是在网关、路由器、防火墙一类的设备处，通常由网络管理员来操作。使用最方便的是在一个以太网中的任何一台上网的主机上。

2. 网络监听的原理

目前很流行的以太网协议的工作方式是：将要发送的数据包发往连接在一起的所有主

机，包中包含着应该接收数据包主机的正确地址，只有与数据包中目的地址一致的那台主机才能接收。但是，当主机工作在监听模式下时，无论数据包中的目的地址是什么，主机都将接收。

在因特网上有很多使用以太网协议的局域网，许多主机通过电缆、集线器连在一起。当同一网络中的两台主机通信时，源主机将写有目的主机地址的数据包直接发往目的主机。但这种数据包不能在 IP 层直接发送，必须从 TCP/IP 协议的 IP 层交给网络接口，即数据链路层，另外，因网络接口无法识别 IP 地址，因此在网络接口数据包中又增加了一部分首部数据帧信息。在首部数据帧中有两个域，分别为只有网络接口才能识别的源主机和目的主机的物理地址。传输数据时，将包含物理地址的数据帧从网络接口发送到物理线路上，最终到达线路上的每一台主机。

当数字信号到达一台主机的网络接口时，正常情况下网络接口读入数据帧，进行检查，如果数据帧中携带的物理地址是自己的或者是广播地址，则将数据帧交给上层 IP 协议软件，否则就将该帧丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。然而，当主机工作在监听模式下时，所有的数据帧都将被交给上层协议软件处理。而且，当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网时，如果一台主机处于监听模式下，它还能接收到发往与自己不在同一子网（使用了不同的掩码、IP 地址和网关）的主机的数据包。也就是说，在同一条物理信道上传输的所有信息都可以被接收到。

另外，现在网络中使用的大部分协议都是很早以前设计的，许多协议的实现都是基于一种非常友好的、通信双方充分信任的基础之上，许多信息以明文发送。因此，如果用户的账户名和口令等信息也以明文的方式在网上传输，而此时一个黑客或网络攻击者正在进行网络监听，只要具有初步的网络和 TCP/IP 协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。同理，正确地使用网络监听技术也可以发现入侵并对入侵者进行追踪定位，在对网络犯罪进行调查取证时获取有关犯罪行为的重要信息，成为打击网络犯罪的有力手段。

3. 网络监听的检测

如果怀疑网络被监听，则可以采用如下方式进行检测。

（1）对于怀疑运行监听程序的机器，用正确的 IP 地址和错误的物理地址 ping，运行监听程序的机器会有响应。这是因为正常的机器不接收错误的物理地址，而处理监听状态的机器能接收，但如果其 IP 协议栈不再次反向检查，就会响应。

（2）向网上发送大量不存在的物理地址包。由于监听程序要分析和处理大量的数据包，会占用很多的 CPU 资源，从而导致性能下降，这样通过比较发包前后该机器的性能即可判断，但是这种方法难度比较大。

（3）使用反监听工具，例如 antisniffer 等进行检测。

4. 网络监听的防范

网络监听本来是为了管理网络，监视网络状态和数据流动情况，但由于它能有效地截获网上的信息，所以也成为黑客常用的一种攻击手段，借以获得用其他方法很难获得的信



息。当黑客成功登录一台网络上的主机，并取得这台主机超级用户的权限后，为了能够夺取网络中其他主机的控制权，往往使用网络监听这种简单且有效的方法。网络监听可以在网上的任何一个位置进行，如局域网中的一台主机或者网关、路由器以及交换设备上。它可以将网络接口设置为监听模式，截获网上传输的信息；但是网络监听仅能用于物理上连接于同一网段的主机，常被用于获取用户口令。

网络监听很难被发现，因为运行网络监听的主机只是被动地接收在局域局上传输的信息，不主动与其他主机交换信息，也没有修改在网上传输的数据包。对网络监听的防范措施如下。

（1）从逻辑或物理上对网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项措施。其目的是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

（2）以交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（称为单播包）还是会被同一台集线器上的其他用户监听到。

因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法监听。当然，交换式集线器只能控制单播包而无法控制广播包和多播包。

（3）使用加密技术

数据经过加密后，通过监听仍然可以得到传送的信息，但显示的是乱码。使用加密技术的缺点是影响数据传输速度以及使用一个弱加密术比较容易被攻破，系统管理员和用户需要在网络速度和安全性上进行折中。

（4）划分 VLAN

运用虚拟局域网 VLAN 技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的入侵。网络监听技术作为一种工具，总是扮演着正、反两方面的角色。对于入侵者来说，最喜欢的莫过于用户的口令，通过网络监听可以很容易地获得这些关键信息。而对于入侵检测和追踪者来说，网络监听技术又能够在与入侵者的斗争中发挥重要的作用。鉴于目前的网络安全现状，我们应该进一步挖掘网络监听技术的细节，从技术基础上掌握先机，才能在与入侵者的斗争中取得胜利。

8.2.4　网络嗅探器 Sniffer

1．什么是 Sniffer

网络嗅探器 Sniffer 是利用计算机的网络接口收集和分析网络数据的工具。嗅探器最早是为网络管理人员配备的工具，有了它网络管理员可以随时掌握网络的实际情况，查找网络漏洞和检测网络性能。例如，当网络性能急剧下降时，可以通过嗅探器分析网络流量，找出网络阻塞的来源。因此，网络嗅探器也可以理解为一个安装在计算机上的监听设备，

可以用来监听计算机在网络上所产生的众多信息，即可以监听计算机程序在网络上发送和接收到的数据。

2．Sniffer 的工作原理

Sniffer 通常是软硬件的结合。数据在网络上是以很小的称为帧的单位进行传输，帧由几部分组成，不同的部分执行不同的功能。帧通过特定的称为网络驱动程序的软件进行成型，然后通过网卡发送到网线上，进而到达其目标主机，在目标主机端执行相反的流程。接收端主机的以太网卡捕获到这些帧，并通知操作系统帧的到达，然后对其进行存储。就是在这个传输和接收的过程中，嗅探器会造成安全方面的问题。

在局域网中与其他计算机进行数据交换时，发送的数据包将被发往所有联在一起的主机，即广播。由于报头中包含目标主机的正确地址，因此只有与数据包中目标地址一致的那台主机才会接收数据包，其他的机器都会将包丢弃。但是，当主机工作在监听模式下时，无论接收到的数据包中目标地址是什么，主机都将其接收下来，然后对数据包进行分析，就得到了局域网中通信的数据。

3．Sniffer 的功能

（1）专家分析系统

专家分析系统 Sniffer 能够监视并捕获所有网络上的信息数据包，同时建立一个特有网络环境下的目标知识库。经过将问题分离、分析和归类，Sniffer 可实时、自动地发出警告，解释问题的性质并提出解决方案。Sniffer 与其他网络协议分析仪最大的差别在于其人工智能专家系统，有了 Sniffer 的专家系统，用户无须知道那些数据包构成的网络问题，也不必熟悉网络协议，更不用去了解这些数据包的内容，便能轻松解决问题。此外，Sniffer 还提供了专家配制功能，用户可以自己设定专家系统判断故障发生的触发条件。Sniffer 能够自动实时监视网络、捕捉数据、识别网络配置，自动发现网络故障并进行报警，它能指出网络故障发生的位置出现在 OSI 的第几层、网络故障的性质、产生故障的可能原因以及为解决故障建议采取的行动。

（2）实时的监控统计和报警

Sniffer 的实时监控统计和报警功能可根据用户习惯以实时数据或图表方式显示统计结果。统计内容包括如下几个方面：

① 网络统计。例如，当前的平均网络利用率、当前的帧数及字节数、总站数和激活的站数、协议类型、当前和总的平均帧长等。

② 协议统计。例如，协议的网络利用率、协议个数、协议的字节数以及每种协议中各种不同类型的帧统计等。

③ 差错统计。例如，错误的 CRC 校验数、发生的碰撞数、错误帧数等。

④ 站统计。例如，接收和发送的帧数、开始时间、停止时间、消耗时间、站状态等。

⑤ 帧长统计。例如，某一帧长的帧所占百分比、某一帧长的帧数等。此外，当网络的某些指标超过规定的极限时，Sniffer 可自动显示或采用有声形式的报警。Sniffer 还可根据网络管理者的要求，自动将统计结果生成多种格式的统计报告，并可存盘或打印输出。

（3）报表生成

Sniffer 报表生成器允许用户创建图形报告。该报告建立在 Sniffer 所收集的网络监控数据基础之上，一些经预先存储的、易于生成的报告可以提供快速显示受监测网段的全部统计数据以及网络层主机、矩阵和协议分配情况。此外，还可提供针对用户网络通信趋势的重要信息，例如用户可评估哪种资源、哪种协议占用了大部分的带宽。这些数据不仅能帮助网络管理者预测额外的带宽需求，还可以帮助用户分配网络资源。Sniffer 报表生成器可以在网络性能下降发展成为严重的网络故障之前，协助用户预测并更正这些问题。

（4）增强功能

① 故障定位及排除

Sniffer 涉及到系统、设备、应用等多个层面，因此将网络性能报告或网络故障准确定位在涉及到（线路、设备、服务器、操作系统、电子邮件）的具体位置，是 Sniffer 提供的基本功能。

② 预防问题

通过在广域网上对网络设备和网络流量实施监控和分析，Sniffer 能够有效预防网络故障的发生，即使在系统出现性能抖动时，Sniffer 也会及时发现，同时建议系统管理员采用正确的处理方法。

③ 优化性能

通过对线路和其他系统进行透视化的管理，用户可利用 Sniffer 管理系统提供的特殊功能对系统性能进行优化。

④ 提供整体网络运行的健康分析及发展趋势分析

Sniffer 可对网络系统的整体运行情况作出长期的健康分析与发展趋势报告，分析系统目前的使用情况，以及对新系统的规划作出精确的报告。

4. Sniffer 的分类

Sniffer 分为软件和硬件两种。软件的 Sniffer 有 Sniffer Pro、Network Monitor、PacketBone 等，其优点是易于安装部署，易于学习使用，同时也易于交流；缺点是无法抓取网络上所有的传输，某些情况下也就无法真正了解网络的故障和运行情况。硬件的 Sniffer 通常称为协议分析仪，一般都是商业性的，价格也比较昂贵，但会具备支持各类扩展的链路捕获能力以及高性能的数据实时捕获分析功能。

5. Sniffer 的扩展应用

（1）专用领域的 Sniffer

Sniffer 被广泛应用于各种专业领域，例如金融信息交换协议 FIX、组播协议 MultiCast、第三代移动通信技术 3G 的分析系统。它可以解析这些专用协议数据，获得完整的解码分析。

（2）长期存储的 Sniffer 应用

由于现代网络数据量惊人，带宽越来越大，采用传统方式的 Sniffer 产品已很难适应这类环境，因此诞生了伴随有大量硬盘存储空间的长期记录设备，例如 nGenius Infinistream 等。

8.3 几种商用入侵检测系统

目前，网络安全的解决主要采取的技术手段有防火墙、安全路由器等，它们对于防止系统非法入侵都有一定的效果。但是它们只是起着防御作用，而计算机系统的安全总是防不胜防的，一旦它们被攻破，则整个系统将会面临瘫痪的危险。因此，仅仅具有这些手段还不足以对付非法攻击。为改变这种被动局面，一个安全的网络系统应该既要有防火墙等防御手段，还需要有能够对网络安全进行实时监控、攻击与反攻击的网络入侵检测系统。下面将介绍几种商用的入侵检测系统。

8.3.1 ISS BlackICE 入侵检测系统

1. BlackICE 简介

BlackICE 软件是由 ISS 安全公司出品的一款著名的入侵检测系统。该软件在 1999 年曾获得了 PC Magazine 的技术卓越大奖。专家对它的评语是：“对于没有防火墙的家庭用户来说，BlackICE 是一道不可缺少的防线；而对于企业网络，它又增加了一层保护措施，但它并不是要取代防火墙，而是阻止企图穿过防火墙的入侵者。”

BlackICE 集成有非常强大的检测和分析引擎，可以识别 200 多种入侵技巧，给予用户全面的网络检测以及系统的保护。该软件还具有灵敏度及准确率高、稳定性出色、系统资源占用率极少的特点，而且它还可以将那些试图入侵的黑客的 NetBIOS（WINS）名、DNS 名或是他目前所使用的 IP 地址记录下来，以便用户采取进一步行动。

近期发布的 BlackICE PC Protection 3.6 拥有强大的检测、分析以及防护功能，而且很容易使用，可以侦察出谁在扫描系统的端口，在非法攻击者攻击用户系统之前拦截，保护系统不受侵害，并收集入侵攻击者的 IP 地址、网络地址、硬件地址，提供日志供用户查看，同时还增加了如下一些新功能：

（1）在设置中增加了应用程序与通信控制的功能条。
（2）可控制应用程序是否在计算机上执行。
（3）可控制哪些应用程序能与 Internet 通信。
（4）扫描系统，检测所有的系统设置改变。
（5）可在事件列表中记录新软件与新通信事件的发生情况。
（6）可以有效预防 DDoS 攻击，是服务器的首选软件防火墙。

2. BlackICE 的工作机制

BlackICE 安装后，以后台服务的方式运行，前端有一个控制台可以进行各种报警和修改程序的配置，界面很简洁。BlackICE 软件最具特色的地方是内置了应用层的入侵检测功能，并且能够与自身的防火墙进行联动，可以自动阻断各种已知的网络攻击行为。

BlackICE 具有强大的网络攻击检测能力，可以说大部分的非法入侵都会被它发现，并采取：严重、危险、可疑和报告这 4 种级别报警（分别用红、橙黄、黄和绿 4 种颜色标识，危险程度依次降低）。同样，BlackICE 对外来访问也设有 4 个安全级别，分别是：信任、谨防、警惕和可疑。

3. BlackICE 的特点

BlackICE 最显著的特点是执行起来性能非常好，即使当网络负载很饱和时仍然能够检测出入侵攻击。但是，由于使用的是智能防御系统，用户设置与管理的功能较少，在安装 BlackICE 时，管理接口相当麻烦，配置选择也不是很多。同时，由于不具备应用程序安全规则等安全防护手段，BlackICE 的报告机制还不太令人满意，基于 Web 的工具难以使用，通信未加密就通过 HTTP 协议在线路上进行传输，非常不安全。

8.3.2 Dragon 入侵检测系统

1. Dragon 简介

Dragon 入侵检测系统专为各种企业量身度造具有各种特殊要求的检测环境——网络安全实时监控、主机组实时监控、客户/服务器管理及各种事件管理，同时兼具强大且开放的签名格式功能、先进的安全监控功能以及超强的集成管理工具等优越功能。在监测系统日新月异的今天，Dragon 入侵检测系统的这些强大功能为企业提供实际可靠的安全保护，使之免受各种恶意攻击，维护企业网络的正常安全运行。Dragon 入侵检测系统具有一套完整的入侵检测方案，与众不同的是，Dragon 入侵检测系统不但可以对企业内网和外网进行检测，而且还可以对企业的外部 Internet 网站进行检测，其保护的是整个网络架构。通过网络探测器就可以进行基于网络的检测，而通过主机探测器则可实现对主机的检测。此外，通过企业管理服务器实现集中式管理监控、分析，生成报表，企业管理服务器还包括高级策略管理功能。

Dragon 入侵检测系统由凯创公司生产的多种安全产品集成，采用了多种检测技术，包括模式匹配、协议解码、异常检测，其安全检测能力是业界领先的。它可以监控网络、服务器和防火墙的行为，记录非正常和恶意操作，并提供丰富的特征库。它的特征检测库是业界最大的，在深度、广度、数量上动态增加特征库，支持防火墙、Web 服务器和其他应用。特征库每周自动更新发布，如果新的威胁出现时，可以立即检测出新的攻击，从而改善整个企业网络的安全性。

在易用性方面，Dragon 入侵检测系统提供了基于 Web 的集中式全企业网络管理功能，并可以通过电子邮件、SNMP 或 SYSLOG 信息定制报警，及时地向用户反映网络状况。值得注意的是，其主机探测器是模块化的，用户可根据实际需要对其进行扩展，不但方便、灵活，而且也节省了资金投入。

对于需要一款完整的入侵检测系统解决方案的企业客户而言，Enterasys 公司的 Dragon 入侵检测系统提供了基于主机和基于网络的入侵检测系统，也提供了一套完整的行政和事

件管理工具，可以满足最大型企业的需要，也可以让最小的企业实现安全管理。可对网络、服务器和防火墙行为进行监控检测，以发现可疑和恶意的行为迹象，并提供综合功能，改善企业网络的安全性。

2. Dragon 的工作机制

Dragon 入侵检测系统包括网络传感器、主机传感器、策略管理器和安全信息管理器 4 部分。各部分的工作原理如下：

（1）Dragon 网络传感器使用了一个新的专利分析运算法则，提高了检测的性能。

（2）Dragon 主机传感器通过一个灵活的模块化架构，为大多数操作系统提供了基于主机的入侵检测。

（3）Dragon 策略管理器可对各种规模的 Dragon 应用进行集中的企业级管理，每日自动更新签名，确保客户应用最新的探测性能。

（4）Dragon 安全信息管理器通过一个集成的监测、分析和报告系统，集中收集所有安全信息，并在高速数据库中对整个企业的各种事件进行规格化，把它们同在网络和主机以及诸如弱点扫描仪、防火墙和网络服务器等其他设备中所探测到的情况进行关联分析。

3. Dragon 的特点

Enterasys 公司的 Dragon 入侵检测系统产品的特点如下：

（1）Dragon 入侵检测系统可以分为 Dragon Sensor、Dragon Squire 和 Dragon Server 三部分。Dragon Sensor 对网络分组进行监控，通常被部署在防火墙系统之前，或是位于网络的关键位置。Dragon Squire 基于主机，实时监控重要的系统文件，能够最大限度地降低系统对服务器性能的影响。Dragon Server 则为 Dragon Sensor 和 Dragon Squire 的安全管理提供方便。Dragon 入侵检测系统适合部署在各种规模的网络环境中。

（2）Dragon 通过命令行方式来执行，只有非常简单的基于 Web 的报告工具。指令集的简单性也允许 Dragon 的用户很方便地定制和产生他们自己的签名。Dragon 能够处理碎片重组。它不仅能够无错地重组碎片，而且即使当网络占用率达 70%～80%时仍然性能不减。如果想要一个简单而又强大的入侵检测功能，并且要求易于增加或修改签名的话，那么 Dragon 是很好的选择。

（3）Dragon 在易于使用和事件可管理性方面完全失败。Dragon 没有提供中央控制台或任何类型的图形化用户界面 GUI 管理工具，其产生的数据冗长而又复杂，很不容易看懂。Dragon 的成熟还需要一个过程。

8.3.3 ISS RealSecure 入侵检测系统

1. RealSecure 简介

ISS 的实时入侵监控器 RealSecure 是业界第一个集成了基于网络和基于主机的入侵检测和响应系统，可以实时监控访问网络和系统的数据包，分析可疑行为，警告安全管理员



或中断攻击连接，保护网络和系统不受攻击，生成详细报表；安全管理人员可以自动地监控网络中的数据流、主机的日志等，对可疑的事件给予检测和响应，在内联网和外联网的主机和网络遭受破坏之前阻止非法的入侵行为。RealSecure 通过以下部件支持开放的网络环境：

（1）检测和标记主机和网络中的可疑行为，并将这种信息反映给唯一的控制台应用软件。

（2）将紧急威胁和低级、中级配置错误区分开，从而最大限度发挥管理员的作用。

（3）适应动态网络需求，RealSecure 引擎和代理能分别放在网络的多个网段中。

（4）可以把入侵检测系统技术扩展到交换的网络环境中。

RealSecure 有 4 种独特的数据资源来保护服务器免受攻击：应用日志文件、操作系统日志文件、关键系统转换文件和对可疑连接的监测。这些数据资源使 RealSecure 代理能判断攻击者是否成功，检测用户行为，提供详细的、可供向法院起诉的信息。基于这些发现，RealSecure 代理通过中止用户进程和挂起用户账号来阻止更深入的攻击。此外，它还可以送出实时警报、日志文件、发出捕获信息和 E-mail 或执行用户定义的行为。

所有 RealSecure 引擎和 RealSecure 代理都要把报告发送给 RealSecure 管理器并由管理器进行配置。这个控制台应用监控任何一个 RealSecure 引擎和代理的组合状态，不管它们运行在 UNIX 上或 Windows NT 上。这样的结果是企业得到了广泛的入侵检测和响应，易于配置并可从一个站点进行管理。RealSecure 管理器还可作为许多网络和系统管理环境的嵌入模块。

2. RealSecure 的工作机制

RealSecure 是一种实时监控软件，其中包含 RealSecure 网络引擎（基于网络的监控器）、RealSecure 系统代理（基于主机的监控器）和 RealSecure 管理器 3 个部件。各部件的工作原理如下：

（1）网络引擎

RealSecure 网络引擎运行在特定的工作站上，提供网络入侵检测和响应。每个网络引擎通过对流动在指定网段上的信息包进行跟踪分析来识别攻击，收集证据来确定是否有非法攻击正在发生。当网络引擎侦测到非法行为，它将立即作出响应，切断非法连接，发送电子邮件或者寻呼机信号，记录事件，重新调整防火墙，或者采取其他用户自定义的行动。另外，网络引擎还可以把警告发送给管理器或第三方管理控制台，以便以后进行进一步的管理和分析。

（2）系统代理程序

RealSecure 系统代理是基于主机的、对 RealSecure 网络引擎起补充作用的构件，它通过分析主机日志来识别并确认攻击是否成功。每个 RealSecure 系统代理安装在一台工作站或主机上，全面检查系统日志，分析是否有网络和安全破坏事件发生。当发现安全破坏事件时，为了防止遭到进一步的攻击，RealSecure 系统代理会及时终止用户进程和停止用户账号；此外，它还能够发送警报、记录时间、关闭陷阱、发送 E-mail 或执行用户预定义的行动。

（3）管理器

所有的 RealSecure 网络引擎和系统代理都要把报告发送给 RealSecure 管理器，并由管理器来对它们进行配置。管理器监控任何来自 Windows NT 和 UNIX 网络引擎和系统代理的报告以及它们的状态。这样管理非常方便，从一个地方就能很容易对它们进行集中的配置和管理。RealSecure 管理器随网络引擎和系统代理一同发布，而且它可作为插件应用于很多不同的网络和系统管理环境。

3. RealSecure 的特点

RealSecure 作为目前最受业界关注的入侵检测系统，具有如下特点。

（1）安全的监控系统：管理控制器、网络引擎和系统代理之间，通过密钥进行加密通信和身份识别。网络引擎在秘密监控方式下不会受到攻击威胁，实现自身的安全。

（2）最小化网络攻击漏洞，在危险发生之前阻止攻击：对网络攻击实时响应，包括切断连接和重新配置防火墙。

（3）能够被用来收集起诉的证据：记录攻击事件，以便于回放。

（4）业界最广泛的攻击模式识别：管理员不需要是安全专家。

（5）内置的报告生成：管理员会快速收到有结构的网络事件的归纳总结。

（6）支持多种网络接口：以太网、快速以太网、令牌环网和 FDDI。

（7）运行在 Windows NT 和 UNIX 平台：使用 RealSecure 无须购买特殊的硬件，它可运行在已有的 Windows NT 和 UNIX 主机上，并具有从一个主控台监控 UNIX 和 Windows NT 引擎的能力。

（8）监控 Windows 的网络和 TCP/IP 传输：微软的 Windows 网络环境支持 RealSecure 监视违反内部安全策略的事件，包括访问重要服务器上的口令文件或未授权读取被保护的共享资源。

（9）对网络传输流无影响：RealSecure 是完全没有妨碍的，不会对网络传输造成任何延迟。这允许企业扩大网络安全监控范围而不会降低网络速度。

RealSecure 最大的不足在于它无法重组破碎的数据包，这是一个较严重的缺陷。此外，它还缺乏对管理器事件窗口中全部事件的清除功能。但综合来看，在检测入侵行为并且成功地阻止这些行为方面，ISS 的 RealSecure 是基于主机检测和基于网络检测技术实现最佳集成的典范。

8.3.4 Snort 入侵检测系统

1. Snort 简介

Snort 是一个轻量级的网络入侵检测系统。所谓的轻量级，是指在检测时尽可能低地影响网络的正常操作。一个优秀的轻量级的 NIDS 应该具备跨系统平台操作、对系统影响最小等特征，并且管理员能够在短时间内通过修改配置进行实时的安全响应，更为重要的是能够成为整体安全结构的重要成员。Snort 作为其典型代表，首先可以运行在多种操作系



统平台，例如 UNIX 系列和 Windows，与很多商用产品相比，它对操作系统的依赖性比较低。其次，用户可以根据自己的需要及时在短时间内调整检测策略。Snort 集成了多种报警机制来提供实时报警功能，其中包括 syslog、用户指定文件、UnixSocket、通过 SMBClient 使用 WinPopup 对 Windows 客户端报警。Snort 填补了 IDS 只有商业入侵检测系统的空白，可以帮助中小网络的系统管理员有效地监视网络流量和检测入侵行为。

2. Snort 的工作机制

Snort 作为一个基于网络的入侵检测系统 NIDS，其工作原理是在基于共享的网络上检测原始的网络传输数据，通过分析捕获的数据包，匹配入侵行为的特征或者从网络活动的角度检测异常行为，进而采取入侵的预警或记录。就检测模式而言，Snort 属于异常检测。从本质上来说，Snort 是基于规则检测的入侵检测工具，即针对每一种入侵行为，都提炼出其特征值并按照规范写成检验规则，从而形成一个规则数据库。其次，将捕获的数据包按照规则库逐一匹配，若匹配成功，则认为该入侵行为成立。

3. Snort 体系结构

Snort 从结构上看，主要分为如下 4 个部分。

（1）Sniffer 即嗅探器，这是 Snort 最初的开发目的。Snort 没有自己的捕包工具，它使用一个外部的捕包程序库 Libpcap 从物理链路上捕包。Libpcap 可以运行在任何一种流行的硬件和操作系统的组合中，这使得 Snort 成为一个真正的与平台无关的应用程序。Snort 按照 TCP/IP 协议的不同层次对收集来的包进行解码，解码后的包数据将堆满一个数据结构。包数据一被存入数据结构中，就会迅速被送到预处理程序和检测引擎中进行分析。

（2）预处理器。以可插入模块的形式存在于 Sniffer 和检测引擎之间。这种插件机制使程序具有很强的扩展性，模块性强，程序易读。Snort 的预处理可以分为两类：一类预处理对发现非基于特征的攻击是不可缺少的；另一类预处理负责对流量标准化，以便检测引擎能准确匹配特征。预处理的参数可以通过 Snort.conf 配置文件调整，还可以根据需要添加或删除预处理程序。

（3）检测引擎。Snort 的核心部件，主要功能是规则分析和特征检测。当数据包从预处理器送过来后，检测引擎依据预先设置的规则检查数据包，一旦发现数据包中的内容和某条规则相匹配，就通知报警模块。启动时，Snort 根据具体的用户需求读取相应的规则文件，并且建立一个三维的链表。当进行规则的匹配时，在链表的两个方向同时进行，检测引擎只检测那些一开始在规则解析器中设置好了的规则选项。当检测引擎检测到第一个与被解码的包相匹配的规则时，检测引擎将触发相应的动作并返回。

（4）日志/报警。检测引擎检查后的 Snort 数据需要以某种方式输出。Snort 对每个被检测的数据包都定义了 3 种处理方式：发送报警信息、记录该数据包和忽略该数据包。这其实是具体定义在检测规则中的。具体工作是在日志/报警子系统中完成的：日志子系统允许用户将包解码收集到的信息以可读的格式或以 Tcpdump 格式记录下来；报警子系统使其将报警信息发送到 syslog、用户指定的文件、UNIX 套接字或数据库中。

4．Snort 的特点

Snort 网络入侵检测系统的特点如下：

（1）Snort 虽然功能强大，但是其代码极为简洁、短小，其源代码压缩包不足 200KB。

（2）Snort 的可移植性非常好。Snort 的跨平台性能极佳，目前已经支持 Linux 系列、Solaris、BSD 系列、IRIX、HP-UX、Windows 系列、ScoOpenserver 和 UnixWare 等。

（3）Snort 具有实时流量分析和进行 IP 数据包日志记录的能力。它能够快速地检测网络攻击，及时地发出警报。Snort 的警报机制很丰富。

（4）Snort 能够进行协议分析、内容的搜索/匹配。它能够检测多种方式的攻击和探测，例如缓冲区溢出、CGI 攻击、SMB 检测、探测操作系统漏洞的企图等。

（5）Snort 的日志格式既可以是 Tcpdump 的二进制格式，也可以编码成 ASCII 字符形式，更便于拥护尤其是新手检查或使用数据库输出插件，Snort 可以把日志记入数据库，当前支持的数据库包括 Postagresql、MySQL、ODBC 和 Oracle 等数据库。

（6）使用 TCP 流插件，Snort 可以对 TCP 包进行重组。Snort 能够对 IP 包的内容进行匹配，但是对于 TCP 攻击，如果攻击者使用一个程序，每次发送只有一个字节的数据包，完全可以避开 Snort 的模式匹配。而被攻击主机的 TCP 协议栈会重组这些数据，将其发送给目标端口上监听的进程，从而使攻击包逃过 Snort 的监视。使用 TCP 流插件，可以对 TCP 包进行缓冲，然后进行匹配，使 Snort 具备对付上面攻击的能力。

（7）使用 SPADE（Statistical Packet Anomaly Detection Engine）插件，Snort 能够报告非正常的可疑包，从而对端口扫描进行有效的检测。

（8）Snort 还有很强的系统防护能力。例如，使用其 IPTables、IPFilter 插件可以使入侵检测主机与防火墙联动，通过 FlexResp 功能，Snort 能够命令防火墙主动断开恶意连接。

（9）扩展性能较好，对于新的攻击威胁反应迅速。

（10）Snort 支持插件，可以使用具有特定功能的报告、检测子系统插件并对其功能进行扩展。Snort 当前支持的插件包括数据库日志输出、破碎数据包检测、端口扫描检测、HTTP URL 以及 XML 网页生成等插件。

（11）Snort 的规则语言非常简单，能够对新的网络攻击做出很快的反应。发现新攻击后，可以很快地根据 Bugtrag 邮件列表，找到特征码，写出新的规则文件。

总之，对于世界上各安全组织来讲，Snort 入侵检测系统都是一个十分优秀的入侵检测系统，它具有小巧灵便、易于配置、检测效率高等优点。下面对 Snort 在 Windows 平台下的安装、配置和使用技术做一简要介绍。

1．Snort 在 Windows 平台下的安装、配置

Snort 可以运行在 UNIX 系统和 Windows 平台上，下面将简要介绍 Windows XP 下 Snort 的安装与配置过程。

（1）双击 WinPcap 安装程序，这里以 WinPcap 4.0.2 为例，安装界面如图 8-5 所示。

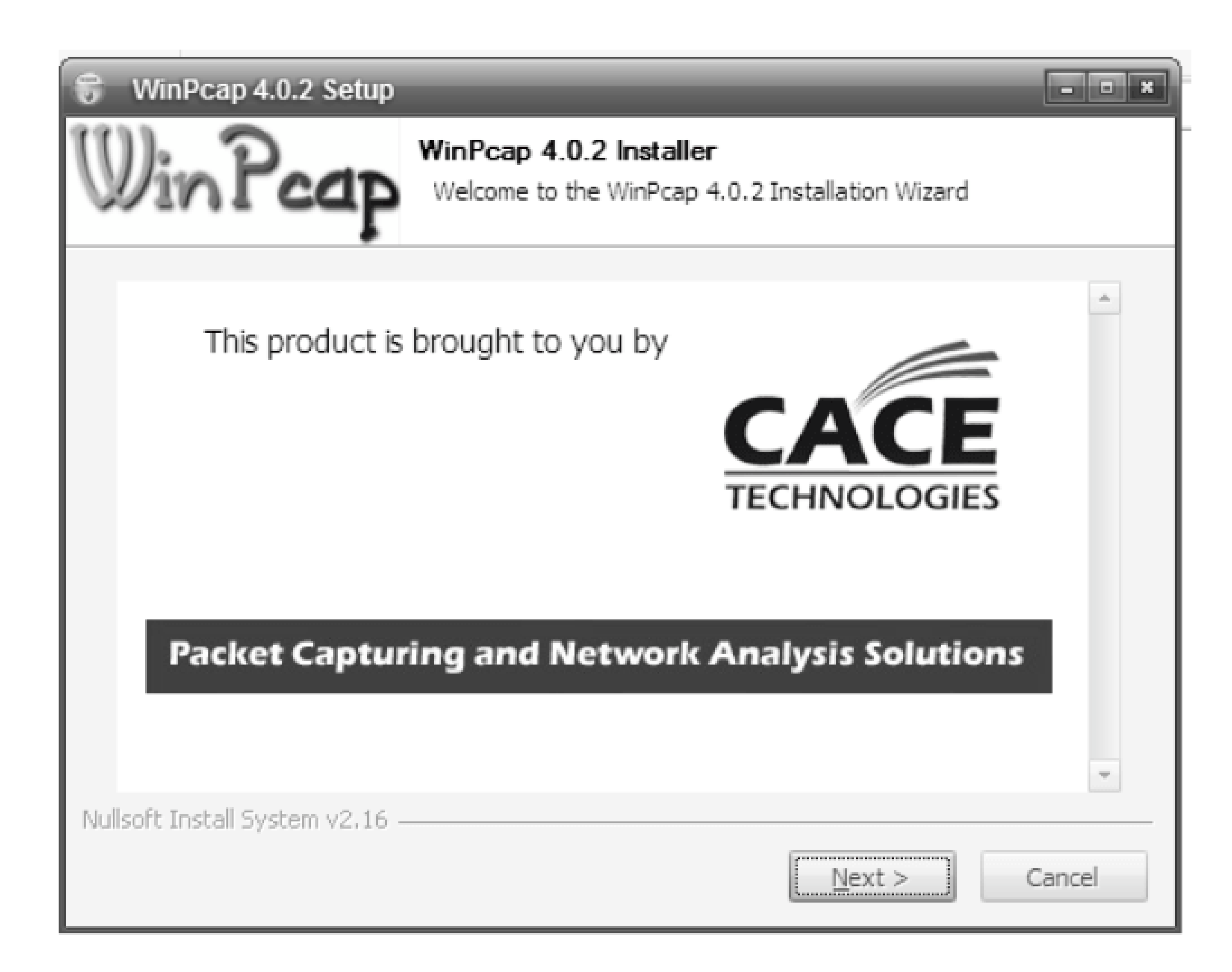


图 8-5　安装 WinPcap 4.0.2

提示：因为需要对网络底层进行操作，安装 Snort 前需要预先安装 WinPcap（Windows Packet Capture Library，Win32 平台上网络分析和捕获数据包的链接库）。

（2）安装完 WinPcap 后，再安装 Windows 平台下的 Snort 安装程序，安装界面如图 8-6 所示，在此选择安装路径为 C:\Snort。



图 8-6　安装 Snort

（3）安装完 Snort 后，在 DOS 命令窗口中执行如下命令：

C:\Snort>cd C:\Snort\bin

C:\Snort\bin>Snort -W

如果安装成功，系统将显示如图 8-7 所示的信息。

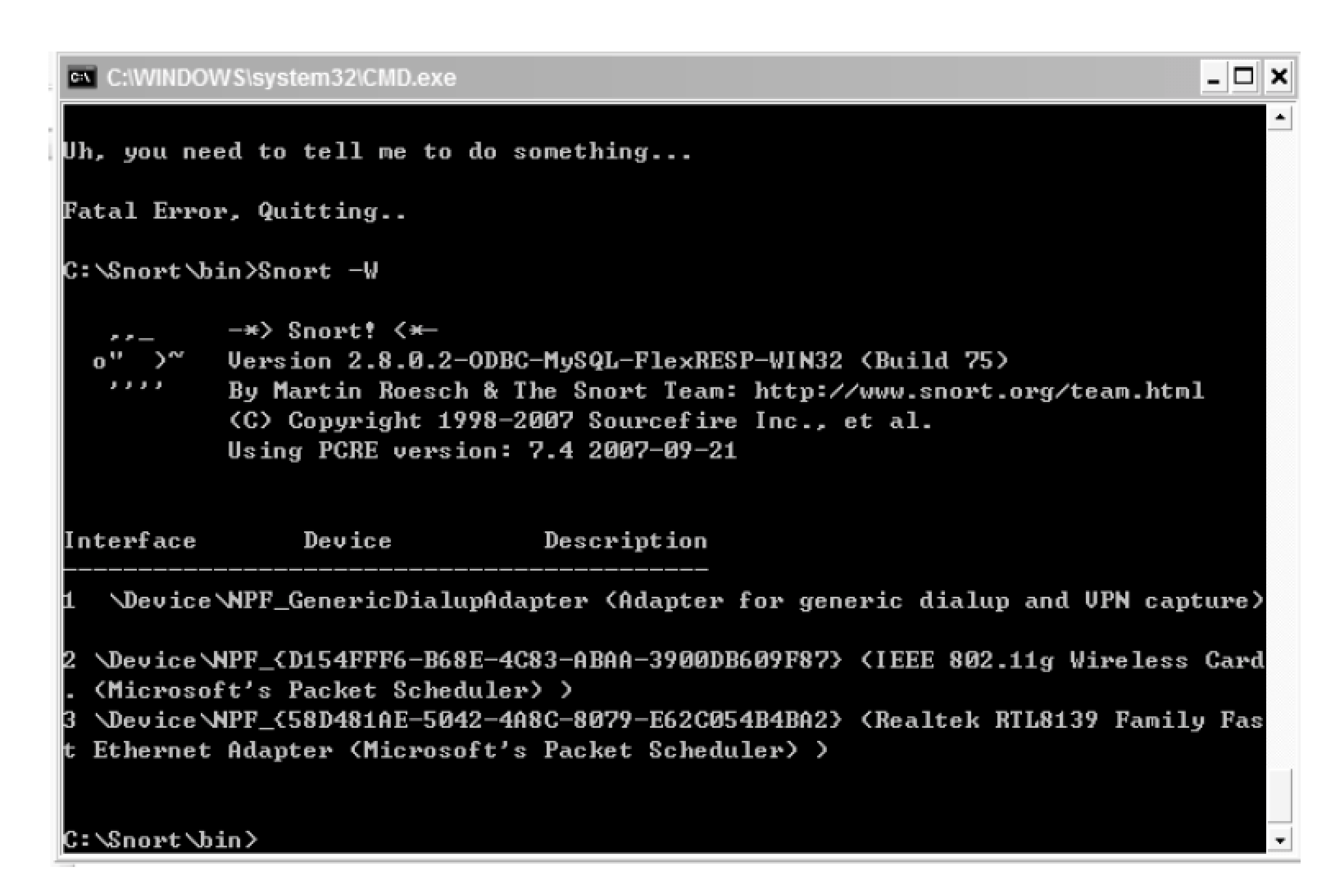


图 8-7 在命令窗口检测 Snort 安装成功

2. Windows 平台下 Snort 的使用

Snort 安装配置完成后，为了进一步查看 Snort 的运行情况，可以人为制造一些 ICMP 网络流量。

（1）如图 8-8 所示，在局域网段的另一台主机（10.110.100.81）上使用 ping 指令，探测运行 Snort 的主机。

```
C:\WINDOWS\system32\cmd.exe
Reply from 10.110.100.33: bytes=32 time<1ms TTL=128
Reply from 10.110.100.33: bytes=32 time<1ms TTL=128
Reply from 10.110.100.33: bytes=32 time<1ms TTL=128
Reply from 10.110.100.33: bytes=32 time<1ms TTL=128

Ping statistics for 10.110.100.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 10.110.100.33

Pinging 10.110.100.33 with 32 bytes of data:

Reply from 10.110.100.33: bytes=32 time<1ms TTL=128
Reply from 10.110.100.33: bytes=32 time<1ms TTL=128
Reply from 10.110.100.33: bytes=32 time<1ms TTL=128
Reply from 10.110.100.33: bytes=32 time<1ms TTL=128

Ping statistics for 10.110.100.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

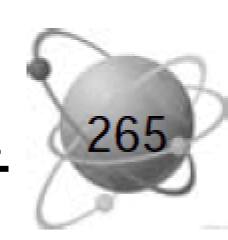
C:\Documents and Settings\Administrator>
```

图 8-8 使用 ping 指令探测主机

（2）回到运行 Snort 的主机（10.110.100.33），使用 Snort 的嗅探器模式输入如下命令。

Snort –v –i3

发现 Snort 已经记录了这次探测的数据包，如图 8-9 所示。



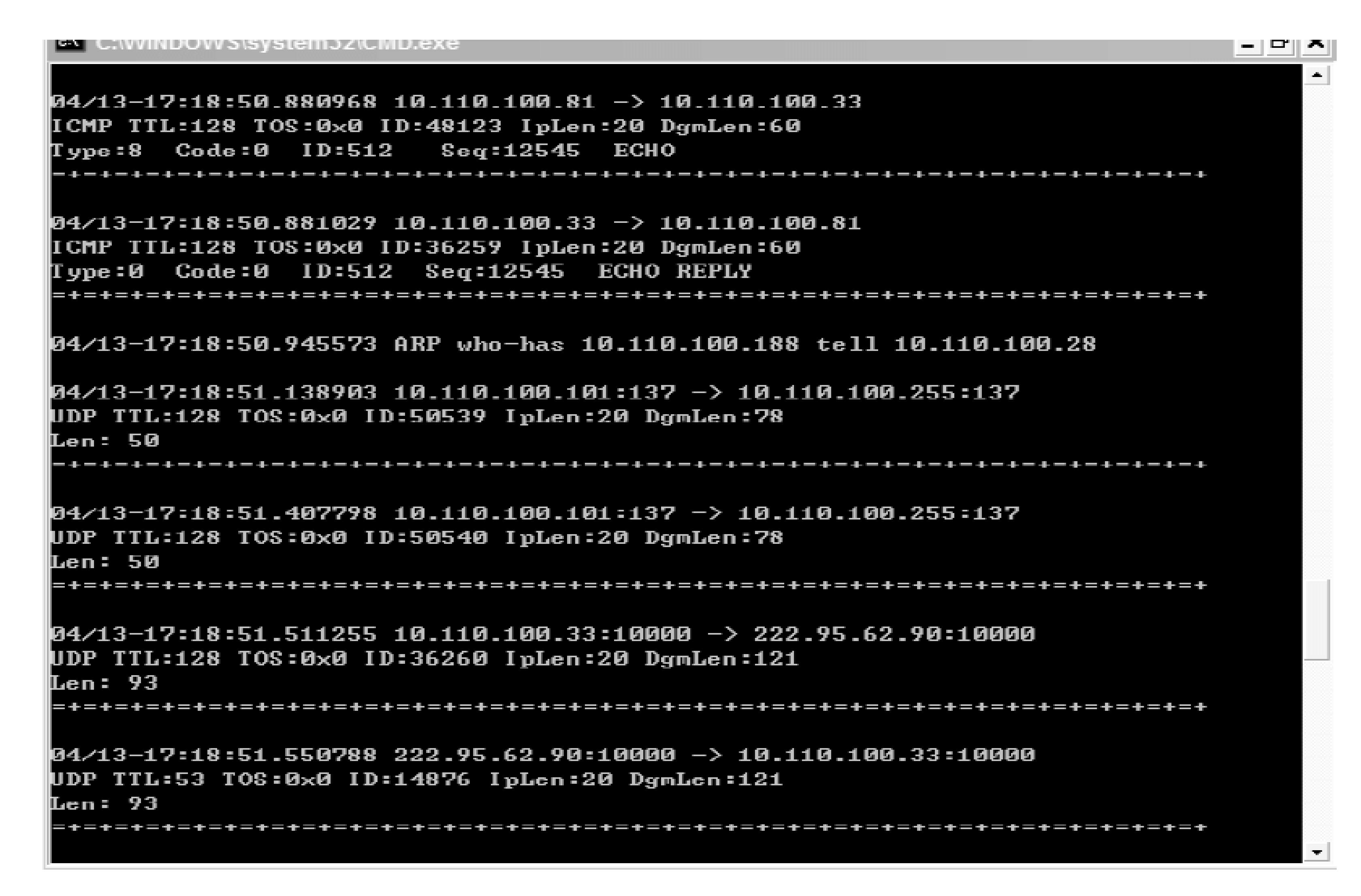


图 8-9　Snort 的嗅探器模式

（3）利用数据包记录模式将屏幕上输出的信息记录在 LOG 日志文件中。输入如下命令启用数据包记录模式：

Snort –dve –i3 –l c:\Snort\log –h 10.110.100.0/24 –K ascii

（4）在命令窗口中运行该命令后，在日志目录 LOG 下将自动生成多个文件夹和文件，如图 8-10 所示。每个文件夹下记录的日志就是和该外部主机相关的网络流量。

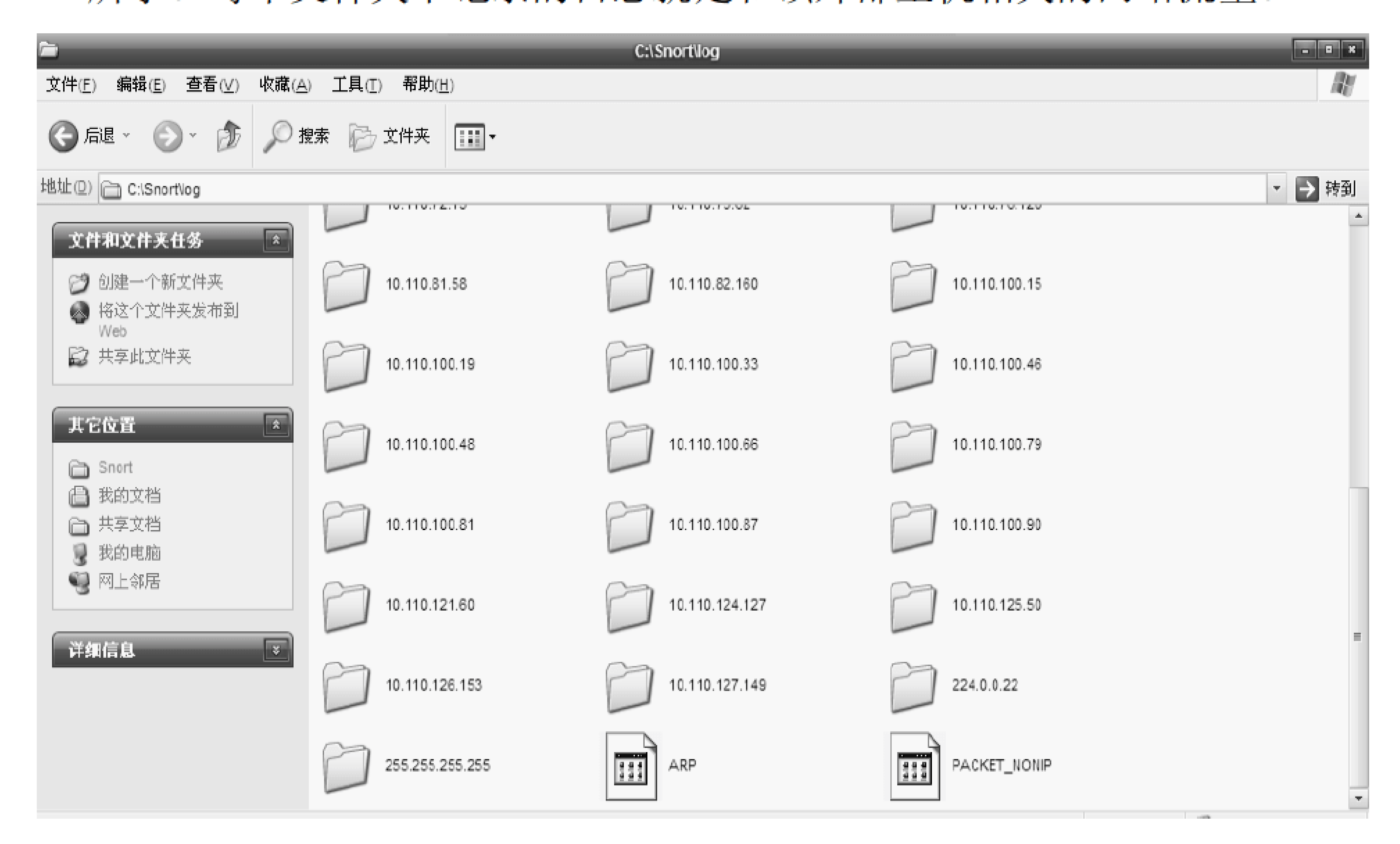


图 8-10　Snort 数据包记录模式记录的日志

（5）打开另一台主机（10.110.100.81）探测目标主机（10.110.100.33 ）产生的日志文件夹，用记事本查看其中的日志文件，会发现文件的内容和嗅探器模式下的屏幕输出类似，如图 8-11 所示。



图 8-11　Snort 数据包记录模式下日志的内容

以上介绍了 Snort 的工作机制、体系结构、特点及其在 Windows 平台下的安装、配置和基本使用方法。Snort 有一组规则，它们详细阐述了各种入侵的特征，使 Snort 能够探测到各种已知的入侵。但由于入侵的类型是不断迅速变化的，因此这些规则必须频繁更改，尽可能保证与最新攻击的各种类型保持一致，使 Snort 始终能通过规则文件检测到入侵的动作。

关于 Snort 规则及其用法，在此不作介绍，读者可自行查阅相关资料。

8.4　IDS 目前存在的问题及其发展趋势

1．IDS 目前存在的问题

入侵检测系统作为一种主动的安全防护技术，能够在网络系统受到侵害之前拦截和响应入侵，为用户提供了对内、外部攻击的实时保护。但是，现在对 IDS 的研究还不够深入，产品的性能也有待于提高。具体来说，IDS 目前存在的主要问题如下。

（1）多数入侵检测系统的体系结构是集中统一收集和分析数据，即数据由单一的主机收集，并按唯一的标准用不同方法进行分析。还有一些 IDS 用多种标准从被监视的多个分布式主机上收集分散的数据，但这些数据仍要由一台完全独立的机器集中进行分析处理。该体系结构存在可扩展性较差、IDS 重新配置或增加困难等问题。绝大多数入侵检测系统的处理效率低下，不能满足大规模和高带宽网络的安全防护要求。

（2）目前使用的主要检测方法是将审计事件同特征库中的特征相比较、匹配，但现在的特征库组织简单，导致的漏报率和误报率较高，很难实现对分布式、协同式攻击等复杂攻击手段的准确检测；此外，预警能力严重受限于攻击特征库，缺乏对未知入侵的预警能力。即使检测到攻击，现有的入侵检测系统的响应能力和实时性也很有限，不能预防现在常见的快速脚本攻击，对于此类快速的恶意攻击只能发现和记录，而不能实时阻止。

（3）中心控制台对攻击数据的关联和分析能力不足，人工参与过多。



（4）系统的自适应能力差，软件的配置和使用复杂，不能自动地适应环境，需要安全管理员根据具体的环境对软件进行复杂的配置。

（5）入侵检测技术及相关标准化仍处于研究与开发阶段。

（6）入侵检测系统的内部各部件缺乏有效的信息共享和协同机制，限制了攻击的检测能力；入侵检测系统之间基本无法协同，甚至交换信息都很难实现，因此要建立一种大型的基于网络的战略安全预警系统是很困难的。

（7）IDS 本身也往往存在着安全漏洞。

- 对 IDS 数据的攻击有：对 IDS 构件之间传输的数据进行加密，插入攻击和逃避攻击。
- 对 IDS 构件的攻击有：冒充控制台关闭分析引擎和对 IDS 的拒绝服务攻击。

由于 IDS 的工作原理实际上是一个监听器，接收网段上的所有数据包，并对其进行分析，与一些已有的特征进行匹配，从而发现攻击，并实施相应的措施；但若使用传输模式进行端到端的加密，则 IDS 无法工作，因为其接收的是加密的数据包。

2. IDS 的发展方向

人们在完善原有技术的基础上，又在研究新的检测方法，例如数据融合技术、主动的自主代理方法、智能技术以及免疫学原理的应用等。其主要的发展方向概括如下：

（1）大规模分布式入侵检测。传统的入侵检测技术一般只局限于单一的主机或网络框架，显然不能适应大规模网络的监测，不同的入侵检测系统之间也不能协同工作，因此必须发展大规模的分布式入侵检测技术。

（2）宽带高速网络的实时入侵检测技术。大量高速网络的不断涌现，各种宽带接入手段层出不穷，如何实现高速网络下的实时入侵检测成为一个现实的问题。

（3）入侵检测的数据融合技术。目前的 IDS 还存在着很多缺陷：首先，目前的技术还不能对付训练有素的黑客的复杂攻击；其次，系统的虚警率太高；最后，系统需要对大量的数据进行处理，非但无助于解决问题，还降低了处理能力。数据融合技术是解决这一系列问题的好方法。

（4）与网络安全技术相结合。结合防火墙、病毒防护以及电子商务技术，提供完整的网络安全保障。

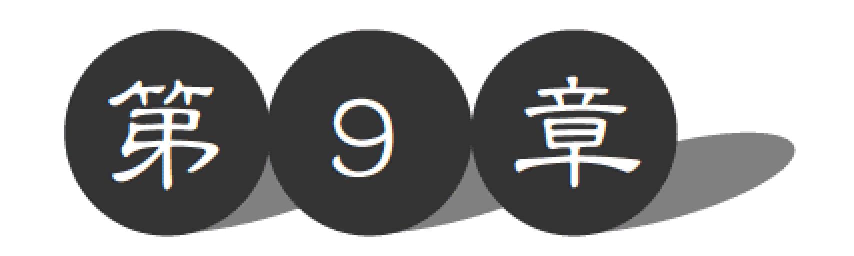
小　结

本章通过介绍网络入侵检测的重要性，描述了入侵检测的结构、原理和检测的过程，并提出了入侵检测的 CIDF 模型。同时，根据检测原理、检测对象、检测系统的体系结构和检测技术的不同，将入侵检测系统划分为不同的类型，提出了评价入侵检测系统的主要性能指标。另外，介绍了入侵检测系统在网络中的典型部署方式、不同的网络扫描技术，以及网络攻击中常用的网络监听技术和 Sniffer 嗅探技术。最后，通过简要介绍 BlackICE、Dragon 和 Snort 3 种商用入侵检测系统的特点及其工作机制，提出了入侵检测系统 IDS 目

前存在的问题及其发展趋势。

练习和思考

1. 简述入侵检测的基本原理和检测过程。
2. 简述入侵检测系统模型 CIDF 的结构。
3. 入侵检测系统有哪些类型？
4. 入侵检测的主要性能指标有哪几项？
5. 网络扫描的主要技术有哪几种？
6. 简述网络嗅探器 Sniffer 的工作原理。
7. 列举几种商用入侵检测系统，并简要介绍其特点。
8. 概述入侵检测的发展方向。



Internet 安全、VPN 和 IPSec

本章学习要求：

（1）掌握 Web 的基本概念和安全需求。

（2）掌握电子商务的基本概念，熟悉安全电子商务体系结构，了解 SSL 和 SET 安全协议。

（3）掌握黑客和网络攻击的概念，熟悉网络攻击的类型和流程，了解相关黑客攻击技术和防范。

（4）熟悉 IPSec 的基本安全技术，掌握 VPN 的基本原理，熟悉 VPN 的应用环境，了解 VPN 协议。

（5）了解电子邮件存在的安全威胁及防范方法，掌握电子邮件加密软件的应用。

（6）了解 TCP/IP 协议，熟悉 TCP/IP 协议的层次安全。

（7）了解 Web 存在的实际安全问题和解决方法。

重点难点：

（1）重点：TCP/IP 协议的层次安全；Web 的安全需求，Web 存在的实际安全问题和解决方法。

（2）难点：VPN 的基本原理；IPSec 的基本安全技术。

Internet 是基于 TCP/IP 协议簇的计算机网络，而 TCP/IP 也是目前 Internet 上最流行的协议。不过，在 Internet 于 1966 年诞生时，创建者更注重的是网络的功能，因此 Internet 和 TCP/IP 协议并没有被过多地考虑安全性。随着 Internet 技术的发展，利用 Internet 进行网上银行、电子购物、电子商务等多种与经济生活相关的经济活动如今早已成为了现实。在此类经济活动中，人们最为关心的问题就是 Internet 的安全性。

Internet 安全协议 IPSec 是 IETF 定义的 Internet 安全通信的一系列规范，为私有信息通过公用网提供了安全保障。IPSec 规范相当复杂，其中包含大量的文档。IPSec 在 Internet 的 IP 层提供安全服务，可使系统按需选择安全协议，决定服务所使用的算法及放置需求服

务所需密钥到相应位置，因此可以有效地保护各种上层协议，并为各种安全服务提供一个统一的平台。IPSec 也是被下一代 Internet 所采用的网络安全协议。

目前，虚拟专用网 VPN 技术也是实现安全传输的重要手段之一，利用它可以在远程用户、公司分支机构、商业合作伙伴与公司的内部网之间建立可信的安全连接，保护数据的安全传输；同时，通过将数据流转移到低成本的 IP 网络上，可以大幅度地减少用户使用 WAN 和远程网络连接的费用。正因为它的安全、节省费用、灵活性大等特点，VPN 得到了迅速的发展，并成为网络技术领域中的一个热点。目前，IPSec 协议是 VPN 开发中使用得最广泛的一种协议，有可能在将来成为 IPVPN 的标准，用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。

本章从 Internet 中最流行的协议——TCP/IP 协议的基本概念出发，着重介绍 TCP/IP 协议的安全性问题、Web 站点安全、虚拟专用网 VPN，以及 Internet 安全协议 IPSec。

9.1 TCP/IP 协议及其安全

TCP/IP 是指传输控制协议/网际协议，是 Internet 上所有网络和主机之间进行交流所使用的共同“语言”，是 Internet 上使用的一组完整的标准网络连接协议。通常所说的 TCP/IP 协议实际上包含了大量的协议和应用，且由多个独立定义的协议组合在一起，因此也称其为 TCP/IP 协议簇。

9.1.1 TCP/IP 的层次结构

TCP/IP 的体系结构比较简单，只有 4 层，分别是网络接口层、网络层、传输层和应用层。

（1）网络接口层。TCP/IP 模型的最低层是网络接口层，也被称为网络访问层，其中包括可使用 TCP/IP 与物理网络进行通信的协议，且对应着 OSI 的物理层和数据链路层。TCP/IP 标准并没有定义具体的网络接口协议，而是旨在提供灵活性，以适应各种网络类型（如 LAN、MAN 和 WAN），这也说明了 TCP/IP 协议可以运行在任何网络之上。

（2）网络层。网络层是在 Internet 标准中正式定义的第一层。网络层所执行的主要功能是处理来自传输层的分组，将分组形成数据包（IP 数据包），并为该数据包进行路由选择，最终将数据包从源主机发送到目的主机。在网络层中，最常用的协议是网际协议 IP，其他一些协议用来协助 IP 协议的操作。

（3）传输层。TCP/IP 的传输层也被称为主机至主机层，与 OSI 的传输层类似，主要负责主机到主机之间的端到端通信。该层使用了两种协议——TCP 与 UDP 来支持两种数据的传送方法。

（4）应用层。在 TCP/IP 模型中，应用程序接口是最高层。与 OSI 模型中的高 3 层任务相同，应用层也是用于提供网络服务，如文件传输服务、远程登录、域名服务和简单网

络管理等。

9.1.2　TCP/IP 的主要协议及其功能

在 TCP/IP 的层次结构中包括 4 个层次，但实际上只有 3 个层次包含了实际的协议。TCP/IP 中各层的协议如图 9-1 所示。

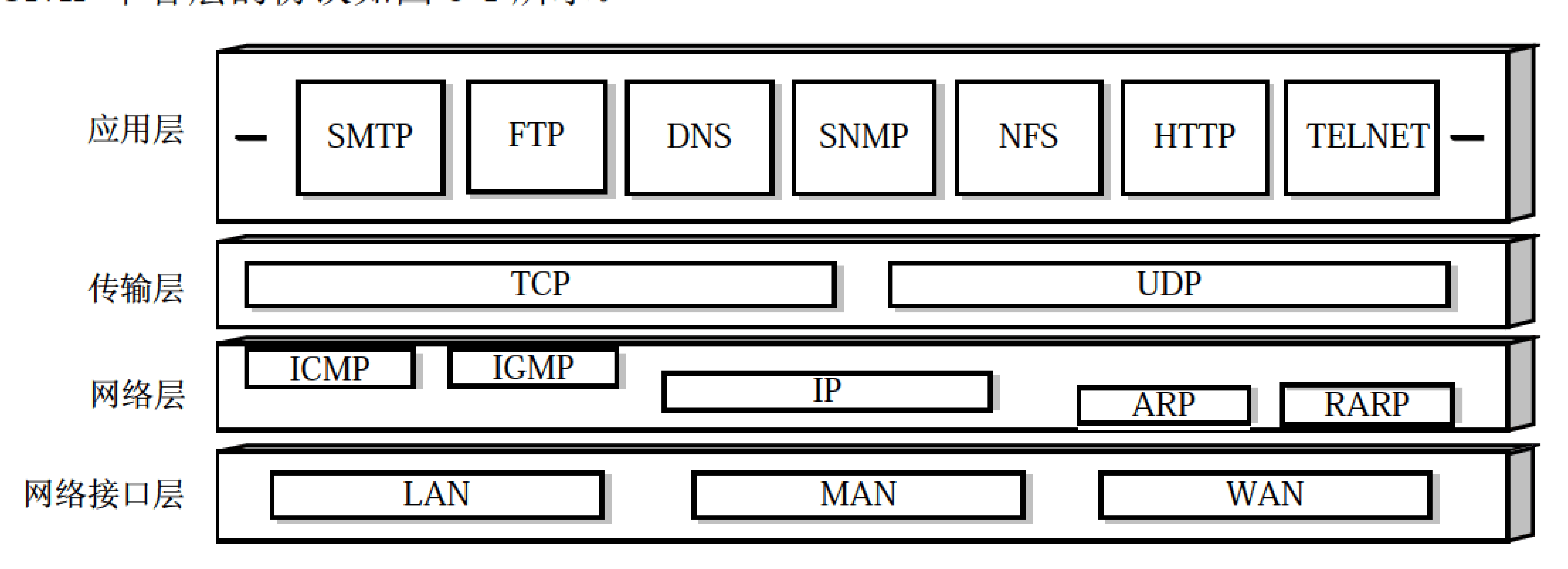


图 9-1　TCP/IP 协议簇

1. 网络层协议

（1）网际协议（Internet Protocol，IP）

IP 协议的任务是对数据包进行相应的寻址和路由选择，并从一个网络转发到另一个网络。IP 协议在每个发送的数据包前都加入了控制信息，其中包含了源主机的 IP 地址、目的主机的 IP 地址和其他一些信息。IP 协议的另一项工作是分割和重编被分割的传输层数据包。由于数据包要从一个网络转发到另一个网络，当两个网络所支持传输的数据包大小不同时，IP 协议就要在发送端将数据包分割，然后在分割的每一段前再加入控制信息进行传输。当接收端接收到数据包后，IP 协议将所有的片段重新组合成原始的数据。

IP 是一个无连接的协议。无连接是指主机之间不建立用于可靠通信的端到端连接，源主机只是简单地将 IP 数据包发送出去，而 IP 数据包可能会丢失、重复、延迟或者次序混乱。因此，要实现数据包的可靠传输，就必须依靠高层的协议或应用程序，例如传输层的 TCP 协议。

（2）网际控制报文协议（Internet Control Message Protocol，ICMP）

网际控制报文协议 ICMP 为 IP 协议提供差错报告。由于 IP 是无连接的，且不进行差错检验，当网络上发生错误时它不能检测错误。此时向发送 IP 数据包的主机汇报错误便成了 ICMP 的责任。例如，如果某台设备不能将一个 IP 数据包转发到另一个网络，它就向发送数据包的源主机发送一个消息，并通过 ICMP 解释这个错误。ICMP 能够报告的一些普通错误类型有：终点不可达、阻塞、时间超时、参数问题、改变路由等。

（3）网际主机组管理协议（Internet Group Management Protocol，IGMP）

IP 协议只负责网络中点到点的数据包传输，而点到多点的数据包传输则要依靠网际主机组管理协议 IGMP 来完成。它主要负责报告主机组之间的关系，以便相关的设备可支持

多播发送。

（4）地址解析协议（Address Resolution Protocol，ARP）和反向地址解析协议（Reverse Address Resolution Protocol，RARP）

计算机网络中各主机之间要进行通信时，必须知道彼此的物理地址。因此，在 TCP/IP 的网络层有 ARP 和 RARP 协议，它们的作用是将源主机和目的主机的 IP 地址与它们的物理地址相匹配。

2．传输层协议

（1）传输控制协议 TCP

TCP 是 TCP/IP 体系中面向连接的传输层协议，可提供全双工的和可靠的交付服务。而对大量数据的传送，一般都要求有可靠的传送。

TCP 协议将源主机应用层的数据分成多个分组，然后将每个分组送到网络层，网络层将数据封装为 IP 数据包，并发送到目的主机。目的主机的网络层将 IP 数据包中的分组传送给传输层，再由传输层对这些分组进行重组，还原成原始数据，并传送给应用层。另外，TCP 协议还要完成流量控制和差错检验任务，以保证数据的可靠传输。

（2）用户数据报协议 UDP

UDP 是一种面向无连接的协议，因此它不能提供可靠的数据传输。UDP 也不进行差错检验，必须由应用层的应用程序来实现可靠性机制和差错控制，以保证端到端数据传输的正确性。虽然 UDP 与 TCP 相比显得不可靠，但在一些特定的情况下还是很有优势的。例如，要发送的信息较短，不值得在主机之间建立一次连接。另外，面向连接通信通常只能在两个主机之间进行，若要实现多个主机之间的一对多或多对多的数据传输，即广播和多播，就需要 UDP 协议。

3．应用层协议

TCP/IP 层次结构中，应用层包括了所有的高层协议，都是为用户或应用程序提供特定网络服务功能来设计和使用的，并且总是随着新业务的增加而不断地有新的协议加入。应用层协议主要有以下几种：

（1）远程终端协议 Telnet：本地主机作为仿真终端登录到远程主机上运行应用程序。

（2）文件传输协议 FTP：实现计算机之间的文件传送。

（3）简单邮件传输协议 SMTP：实现计算机之间电子邮件的传送。

（4）域名服务 DNS：用于实现域名与 IP 地址的映射。

（5）动态主机配置协议 DHCP：实现对计算机的地址分配和配置工作。

（6）路由信息协议 RIP：用于网络设备之间交换路由信息。

（7）超文本传输协议 HTTP：用于 Internet 中的客户机与 WWW 服务器之间的数据传输。

（8）网络文件系统 NFS：实现计算机之间的文件系统共享。

（9）引导协议 BOOTP：用于无盘主机或工作站的启动。

（10）简单网络管理协议 SNMP：实现网络管理。



9.1.3　TCP/IP 的层次安全

基于 TCP/IP 协议的网络安全服务是分层的，不同层次提供的网络服务是不同的，所以提供的安全性也不同。例如，在网络层提供虚拟专用网络，在传输层提供安全套接服务等。

1. 网络接口层安全

网络接口层是 TCP/IP 协议的最低层，包括 OSI 的物理层、数据链路层。从理论上讲，该层并不是 TCP/IP 的一部分，但它是组成 Internet 的各种通信网络（包括局域网 LAN、城域网 MAN、广域网 WAN）与 TCP/IP 之间的接口，是 TCP/IP 实现的基础。为保证通过网络链路传送的数据安全，主要采用划分 VLAN、加密通信等手段。

网络接口层是 TCP/IP 网络中最复杂的一个层次，常见的攻击是针对组成 TCP/IP 网络的以太网进行网络嗅探，即利用网络上的接口接收不属于本机的数据。在以太网中，所有的通信都是广播的，也就是说在同一个网段的所有网络接口都可以访问在物理媒体上传输的所有数据，而每一个网络接口都有一个唯一的硬件地址，这个硬件地址就是网卡的 MAC 地址。在网络上进行数据通信时，信息以数据报的形式传送，其报头包含了目的主机的硬件地址，只有硬件地址匹配的机器才会接收该数据报。然而网络上也存在一些能接收所有数据报的机器（或接口），称为杂错节点。一般情况下，用户账户和口令等信息都是以明文的形式在网络上传输的，所以一旦被黑客在杂错节点上嗅探到，用户就可能遭到攻击，从而遭受难以弥补的损失。针对这一类攻击，通常可采取以下几种防范措施。

（1）网络分段：防止嗅探最有效的手段就是进行合理的网络分段，并在网络中使用交换机和网桥，最理想的情况应使每一台机器都拥有自己的网络段，当然这会相应地增加很多网络建设费用，所以并不现实。可以尽量使相互信任的机器属于同一个网段，并在网段与网段间进行硬件屏障，最大限度地防止嗅探的存在。

（2）加密：对在网络中传送的敏感数据，如用户 ID 或口令等进行加密，一般可以选用 SSH、FSSH 等加密手段。

（3）禁用杂错节点：安装不支持杂错节点的网卡，可以有效地防止嗅探。

2. 网络层的安全性

在过去 20 多年里，业界相继提出了一些方案对网络层的安全协议进行标准化。例如，安全协议 3 号（SP3）就是美国国家安全局以及标准技术协会作为安全数据网络系统 SDNS 的一部分而制定的；网络层安全协议 NLSP 是由国际标准化组织为无连接网络协议 CLNP 制定的安全协议标准；集成化 NLSP（I-NLSP）是美国国家科技研究所提出的包括 IP 和 CLNP 在内的统一安全机制。所有这些提案的共同点多于不同点。事实上，它们用的都是 IP 封装技术。其本质是纯文本的包被加密，封装在外层的 IP 报头里，用来对加密的包进行 Internet 上的路由选择；到达另一端时，外层的 IP 报头被拆开，报文被解密，然后送到收报地点。

Internet 工程任务组 IETF 已经特许 Internet 安全协议 IPSec 工作组对 IP 安全协议 IPSec 和对应的 Internet 密钥管理协议 IKMP 进行标准化工作。IP 安全协议标准化（IPSP）的主

要目的是使需要安全措施的用户能够使用相应的加密安全体制。该体制不仅能在目前通行的 IPv4 下工作，也能在 IP 的新版本 IPng 或 IPv6 下工作。该体制应该是与算法无关的，即使加密算法替换了，也不会对其他部分的实现产生影响。此外，该体制必须能实行多种安全政策，但要避免给不使用该体制的人造成不利影响。按照这些要求，IPSec 工作组制定了相应规范——认证头（Authentication Header，AH）和封装安全有效负荷（Encapsulating Security Payload，ESP）。简言之，AH 提供 IP 包的真实性和完整性，ESP 提供机要内容。关于 AH 和 ESP 将在 9.7 节再作详细介绍。

网络层安全机制的主要优点是其透明性，也就是说，安全服务的提供不需要应用程序、其他通信层次和网络部件做任何改动；而它最主要的缺点是网络层一般对属于不同进程的相应的包不作区别。对所有去往同一地址的包，它将按照同样的加密密钥机制和访问控制策略来处理。这可能导致提供不了所需的功能，也会导致性能下降。针对面向主机的密钥分配问题，RFC 1825 允许（甚至可以说是推荐）使用面向用户的密钥分配，其中不同的连接会得到不同的加密密钥。但是，面向用户的密钥分配需要对相应的操作系统内核进行比较大的改动。

总之，网络层是非常适合提供基于主机对主机的安全服务的。相应的安全协议可以用来在 Internet 上建立安全的 IP 通道和虚拟专用网。例如，利用它对 IP 包的加密和解密功能，可以简捷地强化防火墙系统的防卫能力。

网络层安全性问题的核心在于网络是否能得到控制，目的网站通过对源 IP 进行分析，便能够初步判断来自这一 IP 的数据是否安全，是否会对本网络系统造成危害，来自这一 IP 的用户是否有权使用本网络的数据。一旦发现某些数据来自不可信任的 IP 地址，系统便会自动将来访者拒之门外，并且大多数系统能够自动记录那些曾经造成过危害的 IP 地址，使它们的数据无法造成第二次危害。网络层的主要安全技术包括防火墙技术、IPSec 技术、端口扫描技术及入侵检测技术。

ARP 欺骗就是发生在网络层上的典型安全问题。TCP/IP 中使用的地址解析协议 ARP，是一种将 IP 地址转换为 IP 对应的网卡的物理 MAC 地址的一种协议。在 TCP 网络环境下，一个 IP 包走到哪里，要怎么走是靠路由表定义。但是，当 IP 包到达该网络后，哪台机器响应这个 IP 包却是靠该 IP 包中所包含的物理地址来识别的。在每台主机的内存中，都有一个 ARP 的转换表，它通常是动态的转换表（但在路由选择中，该 ARP 表可以被设置成静态），在主机需要的时候刷新。

入侵实例：假设某台主机的防火墙只对 210.36.80.67 这个 IP 开放 23 号端口，如果用 Telnet 进入这台主机，非法入侵者将设法使其暂时死机，使发送到 210.36.80.67 的 IP 包无法被主机应答，系统开始更新自己的 ARP 对应表并将 210.36.80.67 的项目删去。此时入侵者即可把自己的 IP 改成 210.36.80.67，并发一个 ping（ICMP0）给主机，要求主机更新它的 ARP 转换表。主机找到该 IP 后，将在 ARP 表中加入新的 IP 地址→MAC 地址对应关系，防火墙即失效，入侵的 IP 变成合法的 MAC 地址，即可 Telnet 了。

上述例子中的 ARP 欺骗过程是在同网段发生的，利用交换机、集线器或网桥是无法阻止的；如果 IP 包经过路由器转发，ARP 欺骗配合 ICMP 欺骗将对网络造成更大的危害。在

实际处理中不要把网络安全信任关系建立在 IP 或 MAC 基础上，理想的关系是建立在 IP+MAC（即绑定 IP 地址和 MAC 地址）基础上；设置静态的 MAC 地址→IP 地址对应表，使主机不能刷新设定好的转换表；使用 Proxy 代理 IP 的传输；使用硬件屏蔽主机，设置路由确保 IP 地址能到达合法的路径，例如静态配置路由 ARP 条目；定期检查 ARP 请求，使用 ARP 监视工具。这些都可以防范 ARP 欺骗。

3．传输层的安全性

传输层负责起点到终点的通信。该层有两个广为使用的协议：TCP 和 UDP。TCP 是一个面向连接的协议，它允许从一台主机发出的报文无差错地发往互联网上的其他机器。UDP 是一个不可靠的、无连接协议，用于不需要 TCP 排序和流量控制而是自己完成这些功能的应用程序。它也被广泛地应用于只有一次的客户机/服务器模式的请求/应答查询，以及快速递交更重要的应用程序，例如传输语音或影像。为了向应用层提供可靠的数据传输，TCP/IP 采取了一系列复杂的措施，包括 3 次握手、基于滑动窗口的确认和重传机制、流量控制等，其中主要通过 3 次握手实现 TCP 连接；但是传输层的脆弱性已成为网络协议攻击的主要突破口之一。其漏洞主要有：

（1）TCP 连接的建立与终止。TCP 连接的建立与断开机制保证了传输的可靠性与速度，但是在连接建立过程完成之后，服务器端将不再验证连接的另一方是不是合法的用户，这种脆弱性的直接后果是连接可能被窃取。

（2）TCP 连接请求队列的处理方法看起来很适用于连接的实际情况，但是很容易出现以下现象——如果某一用户不断地向服务器某一端口发送申请 TCP 连接的 SYN 请求包，但不对服务器的 SYN 包发回 ACK 确认信息，则无法完成连接。当未完成的连接填满传输层的队列时，它将不再接受任何连接请求，包括合法的连接请求，这样就可能使服务器端口服务挂起。

（3）TCP 连接的保持。TCP 连接可长期保持的特性，造成当 TCP 连接上很长时间内无数据被传送时，TCP 连接资源的浪费。

由于 TCP/IP 协议本身非常简单，没有加密、身份认证等安全特性，因此要向上层应用层提供安全通信的机制就必须在 TCP 之上建立一个安全通信层次。TCP 连接欺骗（IP 欺骗）就是传输层存在的典型安全问题。

TCP/IP 协议用 IP 地址来作为网络节点的唯一标识，但是 IP 地址是不固定的，这就为 IP 欺骗带来可能。如果攻击方 X 观察到某合法用户 A 停止运行，或通过其他手段使 A 无法响应报文信息，X 就可以冒充 A 向主机 B 发起连接后进行通信。利用 TCP/IP 建立连接的 3 次握手过程就可以改变或伪造一台主机的 IP 地址。假设主机 X 与 A、B 不在同一个子网内，则主机 X 不能检测到来自 B 的数据包，它只有算出 B 的序列号，才能与之创建 TCP 连接。过程描述如下：

X→B：SYN（序列号=ISN1），SRC=A。

B→A：SYN（序列号=ISN2），ACK（应答号=ISN1+1）。

X→B：ACK（应答号=ISN2+1），SRC=A。

同时主机 X 应该阻止主机 A 响应主机 B 的数据包。一旦主机 X 完成了以上操作，它

就可以向主机 B 发送命令。主机 B 误认为命令是由合法主机 A 发来的，将执行这些命令，从而在 X 和 B 之间建立起正式的相互连接。这样，入侵者假扮成目标系统 B 的被信任主机 A，便可对目标系统进行随心所欲的攻击，例如通过远程过程调用 RPC 的形式等。实质上，TCP 连接欺骗的基础是 IP 欺骗。防范 TCP 连接欺骗的方法有：采用地址信任策略、加强用户认证、关闭所有的 RPC 命令等。

网络层安全机制的主要优点是其透明性，即安全服务的提供不要求应用层做任何改动。这对传输层来说是做不到的。原则上，任何 TCP/IP 应用只要应用传输层安全协议（如 SSL 或 PCT），就必定要进行若干修改以增加相应的功能，并使用稍微不同的 IPC 界面。可见，传输层安全机制的主要缺点就是要对传输层 IPC 界面和应用程序两端都进行修改。可是，比起 Internet 层和应用层的安全机制来，这里的修改还是相当小的。另一个缺点是，基于 UDP 的通信很难在传输层建立起安全机制。同网络层安全机制相比，传输层安全机制的主要优点是它提供基于进程对进程的（而不是主机对主机的）安全服务。

4. 应用层的安全性

应用层是 TCP/IP 的最高层，网络在此层向用户提供各种服务，用户则调用相应的程序并通过 TCP/IP 网络来访问可用的服务，与传输层协议交互的应用程序负责接收和发送数据。在这一层中有许多著名协议，例如文件传输协议 FTP、超文本传输协议 HTTP、虚拟终端协议 Telnet、简单邮件传送协议 SMTP 以及域名服务协议 DNS 等，提供的服务主要有文件传输、网页浏览、远程登录、电子邮件、域名解析等。

网络层的安全协议允许为主机（进程）之间的数据通道增加安全属性，这意味着真正的数据通道还是建立在主机（或进程）之间，但却不可能区分在同一通道上传输的具体文件的安全性要求。例如，如果一个主机与另一个主机之间建立起一条安全的 IP 通道，那么所有在这条通道上传输的 IP 包就都要自动地被加密。同样，如果一个进程和另一个进程之间通过传输层安全协议建立起了一条安全的数据通道，那么两个进程间传输的所有消息就都要自动地被加密。

如果确实想要区分具体文件的不同安全性要求，那就必须借助于应用层的安全性。提供应用层的安全服务实际上是最灵活的处理单个文件安全性的手段。例如，一个电子邮件系统可能需要对要发出的信件的个别段落实施数字签名。较低层的协议提供的安全功能一般不会知道任何要发出的信件的段落结构，也就不可能知道该对哪一部分进行签名。只有应用层是唯一能够提供这种安全服务的层次。

例如，S-HTTP 是 Web 上使用的超文本传输协议 HTTP 的安全增强版本，它提供了文件级的安全机制，因此每个文件都可以被设成私人/签字状态。用作加密及签名的算法可以由参与通信的收发双方协商。S-HTTP 提供了对多种单向散列（Hash）函数的支持，例如 MD2、MD5 及 SHA；对多种单钥体制的支持，例如 DES、三元 DES、RC2、RC4 以及 CDMF；对数字签名体制的支持，例如 RSA 和 DSS。

另一个重要的应用是电子商务。为使 Internet 上的信用卡交易安全起见，MasterCard 公司同 IBM、Netscape、GTE 和 Cybercash 一起制定了安全电子付费协议 SEPP，Visa 国际



公司、微软和其他一些公司一起制定了安全交易技术 STT 协议。同时，MasterCard、Visa 国际和微软已经同意联手推出 Internet 上的安全信用卡交易服务，发布了相应的安全电子交易 SET 协议，针对持卡人用其信用卡通过 Internet 进行付费的方法作了具体的规定。这套机制的后台有一个证书颁发的基础结构，提供对 X.509 证书的支持。

例如，当主机需要将一个域名转换为 IP 地址时，它会向某 DNS 服务器发送一个查询请求。同样道理，将 IP 地址转换为域名时，可发送一个反向查询请求。这样，一旦 DNS 服务器中的数据被修改破坏，DNS 欺骗就会产生。因为网络上的主机都信任 DNS 服务器，所以一个被破坏的 DNS 服务器就可以将客户引导到非法的服务器，从而使某个 IP 地址产生 IP 欺骗。防范方法有：直接用 IP 访问重要的服务，这样至少可以避开 DNS 欺骗攻击。这种方式比较简单，但在有的时候却是不现实的；在主机上保留一个域名和相应 IP 地址的数据库，至少要保留信任主机的相关信息；同时使用正向和反向查询（交叉查询）的方法来杜绝攻击的发生。除以上方案之外，最根本的解决办法就是加密所有对外的数据流，对服务器来说就是尽量使用 SSH 之类的带有加密支持的协议，一般用户则应使用 PGP 之类的软件加密所有发到网络上的数据。

9.2　Web 站点安全

Internet 及 Web 已成为许多人日常生活、工作及交流的一种重要工具。由于 Internet 是根据一定的共识进行自制、在全球范围内实现的庞大系统，它并不在法律和政治范围内运行。对于 Web 管理员来说，感触最深的便是由于 Internet 和 Web 技术的开放性和多层次性，决定了 Internet 和 Web 的安全需要格外的关注，确保 Web 安全不是件容易的事。

9.2.1　Web 概述

WWW（World Wide Web）简称 Web，也称为“万维网”，是一个在 Internet 上运行的分布式的信息服务系统，是一个大规模、联机式的信息储藏所。它由遍布全世界的数以万计的 Web 站点（也称网站）组成，而每个 Web 站点都是由一组精心设计制作的 Web 页（Web Page，也称网页，采用 HTTP 语言制作）组成，在万维网中，可以通过超链接非常方便地在 Internet 上从一个站点访问另一个站点，从而主动地按需要获取丰富的信息。

万维网是一个分布式的超媒体系统，是超文本系统的扩充。一个超文本系统由多个信息源（例如网页）链接而成，而这些信息源的数目实际上是不受限制的。利用一个链接可以方便地找到另一个信息源，而这又可以链接到其他的信息源（依此类推）。这些信息源可以位于世界上任何一个接在 Internet 上的超文本系统中。超文本是 WWW 的技术基础。

WWW 服务采用开放式的客户/服务器工作模式，其基本结构分成服务器端、客户机及通信协议 3 个部分。信息资源以网页的形式存储在 Web 服务器中，用户查询信息时执行一个客户端的浏览器程序，向 Web 服务器发出请求，Web 服务器根据客户端的请求内容，将保存在 Web 服务器中的某个网页返回给客户端。浏览器接收到页面后对其进行解释，最终

将图、文、声、像并茂的画面呈现给用户。

1. 服务器（Web 服务器）

服务器所使用的协议中规定了服务器的传输设定、信息传输格式及服务器本身的基本开放结构。这些驻留在服务器上的软件，负责管理汇集于其上的大量信息，并按用户的要求返回相应信息。

2. 客户机（Web 浏览器）

客户机也称 Web 浏览器，用于向服务器发送资源索取请求，并将接收到的信息进行解码和显示。Web 浏览器是客户端软件，负责从 Web 服务器上下载和获取文件，翻译下载文件中的 HTML 代码，进行格式化，根据 HTML 中的内容在屏幕上显示信息。如果文件中包含图像以及其他格式的文件（例如声频、视频、Flash 等），Web 浏览器会作相应的处理或依据所支持的插件进行必要的显示。

3. 通信协议（HTTP 协议）

Web 浏览器与服务器之间遵循 HTTP 协议进行通信传输。超文本传输协议 HTTP 是分布式的 Web 应用的核心技术协议，在 TCP/IP 协议栈中属于应用层。它定义了 Web 浏览器向 Web 服务器发送索取 Web 页面请求的格式，以及 Web 页面在 Internet 上的传输方式。

Web 服务器通过 Web 浏览器与用户交互操作，相互间采用 HTTP 协议进行通信（服务器和客户端都必须安装 HTTP 协议）。Web 服务器也称为 HTTPd 服务器（d 是指 UNIX 系统中的 daemon）。最早的 Web 服务器软件是在 UNIX 系统上发展起来的，有 CERN 和 NCSA 两种类型。现在占据市场份额最大的是 Apache 服务器软件，并且可以在多种环境下运行，例如 UNIX、Linux、Solaris、Windows 等。在 Window 环境下，由于 Microsoft 得天独厚的优势，因而 IIS 成为 Windows NT 及 Windows 下主要的服务器软件。

Web 浏览器软件中，Netscape 的 Web 浏览器 NN（Netscape Navigator）、NC（Netscape Communicator）具有最广泛的系统平台支持，可以在所有平台上运行；Microsoft 的 IE（Internet Explorer）则是 Windows 平台上运行最完美的浏览器软件。

9.2.2 Web 的安全需求

Web 赖以生存的环境包括计算机硬件、操作系统、计算机网络、许多的网络服务和应用，所有这些都存在着安全隐患，最终威胁到 Web 的安全。

Web 的安全体系结构非常复杂，主要包括以下几个方面的需求：

（1）客户端软件（即 Web 浏览器软件）的安全。

（2）运行浏览器的计算机设备及其操作系统的安全（即主机系统安全）。

（3）客户端的局域网 LAN 的安全。

（4）Internet 的安全。

（5）服务器端的局域网 LAN 的安全。

（6）运行服务器的计算机设备及操作系统的安全（即主机系统的安全）。

（7）服务器上的 Web 服务器软件的安全。

对于 Web 服务的安全性，一定要考虑到所有这些方面，因为它们是相互联系的，每个方面都会影响到 Web 服务的安全性，它们中安全性最差的决定了给定服务的安全级别。例如，一台 Web 服务器安装在一台主机上，并使用该主机的操作系统连接到 Internet 上。即使该 Web 服务器程序的安全性很好，如果操作系统上存在安全漏洞，那么 Web 文档也不会被安全地保护，入侵者可以利用操作系统的漏洞来绕过或攻破该 Web 服务器的保护机制，访问 Web 文档。

了解 Web 的安全需求是实现 Web 安全的第一步，清楚需要保护的对象，才能有的放矢地采取防范措施，实现 Web 的保护。

下面将从 3 个方面分析 Web 的安全需求：

- Web 服务器的安全需求。
- Web 浏览器的安全需求。
- Web 传输过程中的安全需求。

1. Web 服务器的安全需求

随着开放系统的发展和 Internet 的知识普及，获取使用简单、功能强大的系统安全攻击工具变得非常容易。在访问 Web 站点的用户中，不少技术高超的人拥有足够的经验和工具来探视他们感兴趣的东西，而普通用户需要的则是真正的安全系统。不同的网站有不同的安全需求。一般而言，建立 Web 站点是为了更好地提供信息和服务，其安全需求主要包括以下几个方面。

（1）维护 Web 信息的真实性和完整性

这是 Web 服务器最基本的要求。Web 服务器在一定程度上是站点拥有者的代言人，代表拥有者的形象。通过 Web 公布的信息都是经过精心挑选和组织的，如果被人篡改，不仅会使信息遭到破坏，无法实现提供信息或服务的初衷，影响正常的业务，甚至会误导用户，挑起用户和站点拥有者之间的矛盾，严重损害拥有者的形象和声誉。因此必须采取适当的保护措施，对各类用户访问 Web 资源的权限进行严格管理。

（2）维持 Web 服务的可用性

这是为了确保 Web 服务的有效性。一方面要确保用户能够获得 Web 服务，为此要保证运行 Web 服务的设备和操作系统正常运行，Web 服务处于激活状态，同时要采取积极主动的预防、检测措施，防止被人恶意破坏，造成设备、操作系统停运或服务中止；另一方面要确保所提供的服务是可信的，尤其是金融或电子商务站点，为此必须提供必要的相互认证手段的信息保密方法，否则即使 Web 服务随时可供使用也没人敢用，或者由于虚假交易而令商家、客户遭受损失。

（3）保护 Web 访问者的隐私

保护用户的隐私是取信于用户的前提。通常 Web 服务器会对每次连接进行日志记录，另外有些站点的服务仅提供给经过登记的用户，所以 Web 服务器中大多存有用户的个人信息及其有关说明，例如用户的 IP 地址、电子邮件地址、所使用计算机的名称、单位名称

及其简要说明、所访问的页面内容、访问时间、传输数据量、甚至个人信用卡号码等机密信息。

站点可以把这些信息用于商业目的以便从中获利，或用于宣传站点，扩大影响。虽然目前没有明确的法律条文禁止这样做，但是显然这种做法不太符合道德规范，相信大多数网民都不会欢迎突如其来的广告或其他陌生邮件，除非他事先主动选择了这一服务。所以，只有尊重用户隐私并采取适当保护措施的网站才能赢得用户。

（4）确保 Web 服务器不被用作跳板来进一步侵入内部网络或其他网络

首先，Web 服务器不能被作为"跳板"来进一步侵入内部网络系统；其次，要保证 Web 服务器不被用作"跳板"来进一步危害其他网络。这是 Web 服务器最基本的要求，也是服务器保护自己和 Web 浏览器用户的最基本条件。

2．Web 浏览器的安全需求

Web 浏览器为用户提供了一个简单、实用而且功能强大的图形化界面，使得用户能够轻松自如地在网络的海洋里冲浪。但是，使用浏览器的用户也可能遇到一系列的安全问题。当用户点击鼠标，一张张精彩的网页出现在计算机屏幕上的同时，浏览器程序极有可能已经把某些信息传送给网络上的某一台计算机（可能在世界的某一个角落），浏览器向它索取网页，网页通过网络传到浏览器所在的计算机中。返回来的内容，有的是浏览器用户需要的，能够看到的，但是同时还有浏览器不能显示的内容，悄悄地存入浏览器所在计算机的磁盘。这些不显示的内容，可能是协议工作内容，对用户是透明的，但也可能是恶作剧代码，或者是蓄意破坏的代码，它们会窃取 Web 浏览器用户计算机上所有可能的隐私、破坏计算机设备，甚至诱导用户在网上冲浪时误入歧途。因此，注意 Web 浏览器的安全保障也是十分重要的。

一般情况下，用户使用 Web 浏览器获取信息时，安全需求有以下几个方面。

（1）确保运行浏览器的系统不被病毒或者其他恶意程序侵害而遭受破坏。

（2）确保个人安全信息不外泄。

（3）确保所交互的站点的真实性，以免被骗，遭受损失。

3．Web 传输过程中的安全需求

所有信息要想交换，必须在网络上进行传输，因此传输的过程也就成为 Web 安全至关重要的一个环节。Web 浏览器和 Web 服务器之间的信息交换也是通过网络传输来实现的，所以 Web 数据传输过程的安全性直接影响着 Web 的安全。因特网上传输的信息，尤其是远程用户向 Web 服务器传输的交易信息（例如，信用卡信息）如被非法截获，后果不堪设想。此时可以通过数字签名技术，使消息的发送者和接收者在交换信息时都承认参加了信息的交换，当接收者知道发送者签署了交易合同时，应当确信该交易是可靠的。此外，对在因特网上传送的信息必须加密，以防止他人偷看，并确保信息不会被改变，直到信息到达目的地。必须保证用户和 Web 服务器传送的信息没有被泄露或篡改，这一点在经济交易时尤为重要。

不同的 Web 应用对于传输有着不同的要求，但一般都包括如下几个方面。



（1）保证传输方所发信息的真实性：要求所传输的数据包必须是发送方发出的，而不是他人伪造的。

（2）保证传输信息的完整性：要求所传输的数据包完整无缺，当数据包被删节或被篡改时，有相应的检查方法。

（3）安全性较高的 Web 需要保证传输的保密性：敏感信息必须采用加密方式传输，防止被截获而泄密。

（4）认证应用的 Web 需要保证信息的不可否认性：对于那些身份认证要求较高的 Web 应用，必须有识别发送信息是否为发送方所发的方法。

（5）对于防伪要求较高的 Web 应用，要保证信息的不可重用性：尽量做到信息即使被中途截取，也无法被再次使用。

9.3　Web 电子商务安全

电子商务（Electronic Commerce，EC）包含两方面内容：一是电子方式；二是商贸活动。简单来说，电子商务指的就是利用简单、快捷、低成本的电子通信方式，买卖双方不见面地进行各种商贸活动。

电子商务可以通过多种电子通信方式来完成。简单的，例如通过打电话或发传真的方式来与客户进行商贸活动，似乎也可以称为电子商务；但是，现在人们所探讨的电子商务主要是通过电子数据交换 EDI 和 Internet 来完成的。尤其是随着 Internet 技术的日益成熟，电子商务真正的发展将是建立在 Internet 技术上的。所以，也有人把电子商务简称为 IC（Internet Commerce）。

从贸易活动的角度分析，电子商务可以在多个环节实现，由此也可以将电子商务分为两个层次。较低层次的电子商务有电子商情、电子贸易、电子合同等；最完整的也是最高级的电子商务应该是能够利用 Internet 进行全部的贸易活动，即在网上将信息流、商流、资金流和部分的物流完整地实现，也就是说，可以从寻找客户开始，一直到洽谈、订货、在线付（收）款、开具电子发票以至到电子报关、电子纳税等通过 Internet 一气呵成。Internet 的资源共享、快速、便捷是电子商务迅速发展的原因，而 Internet 的开放性却使电子商务在安全方面存在着先天不足。目前，电子商务安全问题变得越来越突出，已经成为制约电子商务快速发展的障碍。

9.3.1　电子商务的安全要求

电子商务所面临的威胁的出现导致了对电子商务安全的需求，也是真正实现一个安全电子商务系统所要求做到的各个方面，主要包括机密性、完整性、认证性和不可抵赖性。

1．真实性

真实性是指网上交易双方身份及交易信息要真实有效。双方交换信息之前要通过数字

签名、身份认证及数字证书等辨别参与者身份的真伪，防止伪装攻击。交易时，对提供的交易信息也要保证其真实性，防止欺骗交易行为。

2. 机密性

电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务是建立在一个较为开放的网络环境上的(尤其 Internet 是更为开放的网络)，维护商业机密是电子商务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。机密性一般通过密码技术来对传输的信息进行加密处理来实现。

3. 完整性

电子商务简化了贸易过程，减少了人为的干预，但同时也带来了维护贸易各方商业信息的完整、统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传输过程中信息的丢失和重复并保证信息传送次序的统一。完整性一般可通过提取信息摘要的方式来获得。

4. 不可否认性

电子商务可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是进行交易所期望的贸易方这一问题则是保证电子商务顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。在无纸化的电子商务方式下，通过手写签名和印章进行贸易方的鉴别已是不可能的。因此，要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。不可否认性可通过对发送的消息进行数字签名来获取。

5. 有效性

电子商务以电子形式取代了纸张，那么如何保证这种电子形式的贸易信息的有效性则是开展电子商务的前提。电子商务作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、确定的地点是有效的。

9.3.2 安全电子商务的体系结构

电子商务的安全体系结构是保证电子商务信息安全的基础。它由 5 个部分组成，具体如图 9-2 所示。

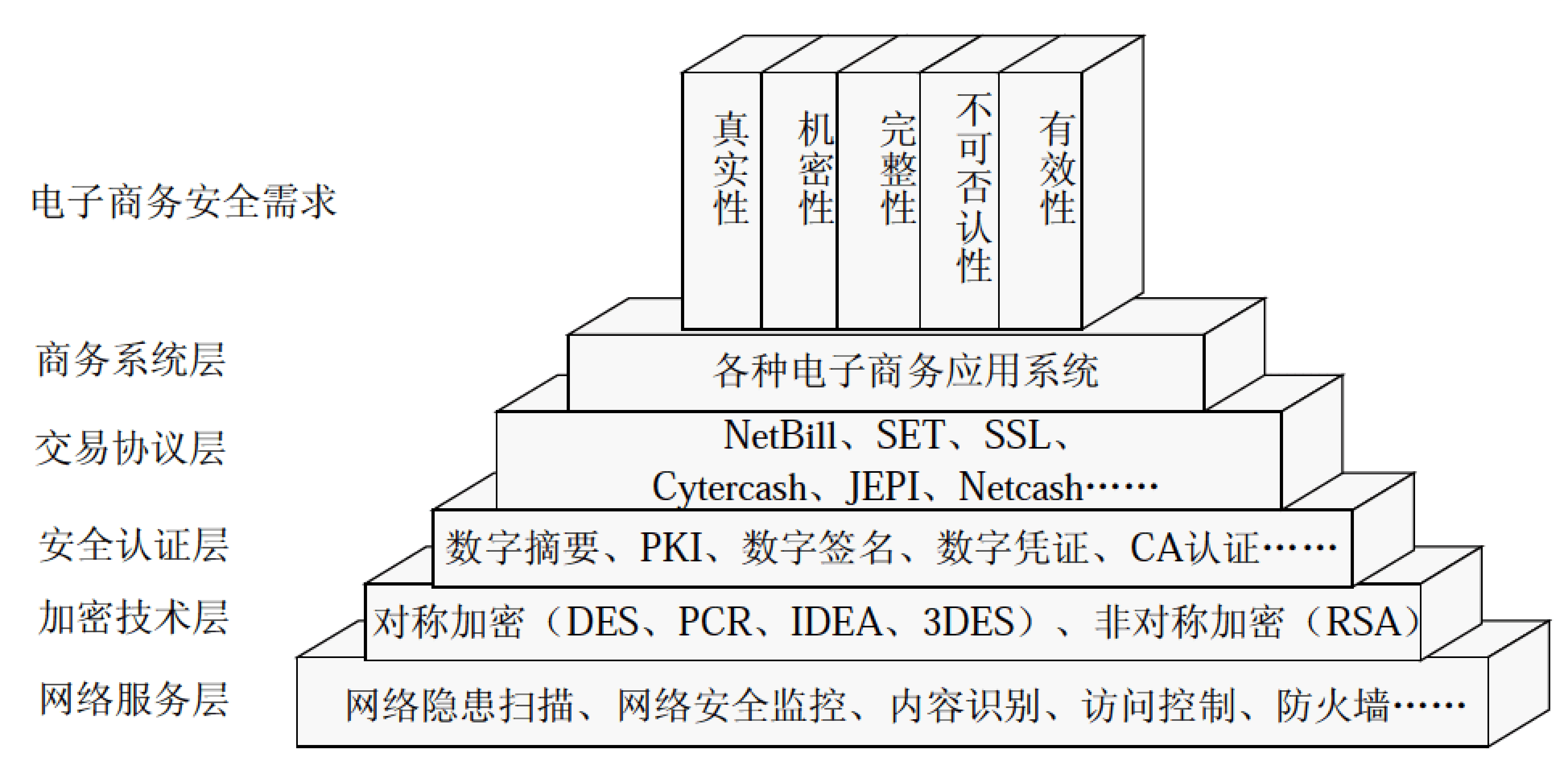


图 9-2　安全电子商务体系结构

1．网络服务层

电子商务系统是依赖网络实现的商务系统。网络服务层是电子商务系统基本的网络服务平台，其中包括网络隐患扫描、网络安全监控、内容识别、防火墙、用户接口和访问控制等模块。其功用是加强网络之间的访问控制，提供安全通信服务平台，防止非法用户以非法手段进入内部网络，非法扫描、访问内部网络资源。

2．加密技术层

加密技术层主要提供对称加密和非对称加密服务，保证商务信息的机密性、真实性。其原理是，将被传输的商务信息（称为明文）变换成难以识别和理解的密文，再传输；同时在接收方进行相应的逆变换（称为解密），从密文中还原出明文，以供本地的信息处理系统使用。商务信息的安全性依赖于使用的算法和密钥的长度。

除了数据加密技术，常见的还有对通信线路加密的链路加密技术和对存储在节点内的文件、数据库信息进行加密保护的节点加密技术等。

3．安全认证层

在安全认证层，主要是通过数字摘要、数字签名、数字证书和 CA 认证等技术去验证商务信息和商务对象的真实性和不可否认性。

数字签名基于非对称加密技术，将数字摘要（MAC）用发送者的私钥加密，与原文一起传送给接收者，接收者只有用发送者的公钥才能解开被加密的数字摘要。数字签名技术主要应用于电子商务安全服务中的源鉴别、完整性服务和不可否认服务。

数字证书又称数字凭证，是用来证实用户的身份、对网络资源的访问权限等的电子手段，包含着标识证书持有者身份的有关信息。数字证书的内容格式由 CCITT X.509 国际标准规定，通常包括证书所有者的姓名、证书所有者的公共密钥、证书的有效期、颁发数字证书的单位名称、数字证书的序列号及颁发数字证书单位的数字签名等内容。

电子商务认证中心 CA，具有网上安全电子交易认证服务、签发数字证书并确认用户身份的功能，负责数字证书的申请、发放和管理，具有证书发放、证书更换、证书撤销、证

书验证四大职能。

4. 交易协议层

交易协议层提供了电子商务封装数据的公平交换服务。目前比较成熟的协议有 Netbill、SET、SSL、Cybercash、JEPI、Netcash 等。不同交易协议的复杂性、开销和安全性各不相同，不同的应用环境对协议的目标要求也不尽相同。

安全套接层 SSL 协议是目前使用最广泛的电子商务协议。该协议由 Netscape 公司研制开发，向基于 TCP/IP 的客户端和服务器应用程序提供了客户端和服务器的鉴别、数据完整性及信息保密性等安全措施。该协议通过在应用程序进行数据交换前先交换 SSL 初始握手信息来实现有关安全特性的审查，从而确保其机密性与数据的完整性。该协议已成为事实上的工业标准。

安全电子交易协议 SET 是一个能保证通过开放网络进行安全资金支付的技术标准，向基于信用卡进行电子化交易的应用提供了实现安全措施的规则。它包含了信用卡在电子商务中的交易协议、信息保密、资料完整及数字认证、数字签名等，验证商家和持卡者，保证信息的保密性、支付的完整性。SET 协议要达到 5 个目标：保证电子商务参与者信息的相应隔离；保证信息在互联网上安全传输，防止数据被黑客或被内部人员窃取；解决多方认证问题；保证网上交易的实时性，使所有的支付过程都是在线的；规范协议和消息格式，促使不同厂家开发的软件具有兼容性与交互操作功能，并且可以运行在不同的硬件和操作系统平台上。

5. 商务系统层

商务系统层主要是提供商业解决方案，例如 B2B、B2C 等各种电子商务应用系统。商务系统层在整个体系结构中处于最上层，其功用是根据电子交易要求，为客户提供全新的功能，包括内容管理、市场推广、订购管理、支付管理等，实现全方位商务活动的数字自动化。

电子商务作为全球商务发展的趋势，给全球的经济、政治和法律带来了深刻的影响。随着电子商务的发展、电子交易手段的多样化，安全问题将会变得更加重要和突出。开展电子商务安全问题的进一步研究，开发我国自己的网络安全产品，对保障我国电子商务的正常发展不仅具有重要的理论价值，而且具有更为重要的现实意义。

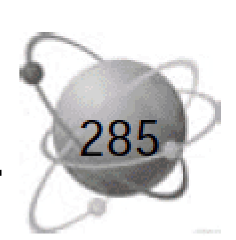
9.3.3 电子商务中的主要安全协议

从电子商务的安全体系结构中可以看出，在其交易协议层中应用了较多的安全协议，这里主要介绍常用的 SSL 和 SET 两种安全交易协议。

1. 安全套接层 SSL 和传输层安全 TLS 协议

1）SSL 简介

安全套接层（Secure Socket Layer，SSL）协议是一种开放性协议，提供了一种介于应用层和传输层之间的数据安全套接层协议机制。它为 TCP/IP 连接提供了数据加密、服务器认证、消息完整性，以及可选的客户机认证。SSL 是在 Internet 基础上提供的一种保证私密



性的安全协议，可使客户机/服务器应用之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户机进行认证。SSL 协议要求建立在可靠的传输层协议（例如，TCP）之上，其优势在于它是与应用层协议独立无关的，应用层协议（例如，HTTP、FTP、Telnet 等）能透明地建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商，以及服务器认证工作。在此之后，应用层协议所传送的数据都会被加密，从而保证通信的私密性。

SSL 协议提供的安全信道具有以下 3 个特性：

① 私密性：在握手协议定义了会话密钥后，所有的消息都被加密。

② 确认性：尽管会话的客户端认证是可选的，但是服务器端始终是被认证的。

③ 可靠性：传送的消息包括消息完整性检查（使用 MAC）。

2）SSL 的结构

SSL 的设计目标是在 TCP 基础上提供一种可靠的端到端安全服务，其服务对象一般是 Web 应用。在 SSL 的体系结构中包含两个协议子层，其中底层是 SSL 记录协议层（SSL Record Protocol Layer）；高层是 SSL 握手协议层（SSL Handshake Protocol Layer）。SSL 的协议栈如图 9-3 所示。

握手	密码参数修改	报警	应用数据（HTTP）
SSL记录协议			
TCP			
IP			

图 9-3　SSL 的协议栈

（1）SSL 记录协议

在 SSL 协议中，所有的传输数据都被封装在记录中。记录是由记录头和长度不为 0 的记录数据组成的。所有的 SSL 通信包括握手消息、安全空白记录和应用数据都要使用 SSL 记录协议层。SSL 记录协议包括了记录头和记录数据格式的规定。

① SSL 记录头格式

SSL 的记录头可以是 2 个或 3 个字节长的编码。SSL 记录头中包含记录头的长度、记录数据的长度、记录数据中是否有粘贴数据等信息。其中粘贴数据是用来在使用块加密算法时，填充实际数据，使其长度恰好是块的整数倍。最高位为 1 时，不含有粘贴数据，记录头的长度为 2 个字节，记录数据的最大长度为 32767 个字节；最高位为 0 时，含有粘贴数据，记录头的长度为 3 个字节，记录数据的最大长度为 16383 个字节。

当数据头长度是 3 个字节时，次高位有特殊的含义。次高位为 1 时，标识所传输的记录是普通的数据记录；次高位为 0 时，标识所传输的记录是安全空白记录（被保留用于将来协议的扩展）。

② SSL 记录数据格式

SSL 的记录数据包含 3 个部分：MAC 数据、实际数据和粘贴数据。

MAC 数据用于数据完整性检查。计算 MAC 所用的散列函数由握手协议中的 CIPHER-CHOICE 消息确定。若使用 MD2 和 MD5 算法，则 MAC 数据长度是 16 个字节。当会话的

客户端发送数据时，密钥是客户的写密钥（服务器用读密钥来验证 MAC 数据）；而当会话的客户端接收数据时，密钥是客户的读密钥（服务器用写密钥来产生 MAC 数据）。序号是一个可以被发送和接收双方递增的计数器，每个通信方向都会建立一对计数器，分别被发送者和接收者拥有。计数器有 32 位，计数值循环使用，每发送一个记录，计数值递增一次，序号的初始值为 0。

（2）SSL 握手协议

SSL 握手协议层包括 SSL 握手协议（SSL Handshake Protocol）、SSL 密码参数修改协议（SSL Change Cipher Spec Protocol）、应用数据协议（Application Data Protocol）和 SSL 报警协议（SSL Alert Protocol）。握手协议层的这些协议用于 SSL 管理信息的交换，允许应用协议传送数据之前相互验证，协商加密算法和生成密钥等。

SSL 握手协议包含两个阶段，第一个阶段用于建立私密性通信信道，第二个阶段用于客户认证。

第一阶段是通信的初始化阶段，通信双方都发出 HELLO 消息。当双方都接收到 HELLO 消息时，就有足够的信息确定是否需要一个新的密钥。若不需要新的密钥，双方将立即进入握手协议的第二阶段；否则，服务器端的 SERVER-HELLO 消息将包含足够的信息（包括服务器所持有的证书、加密规约和连接标识）使客户端产生一个新的密钥。若密钥产生成功，客户端发出 CLIENT-MASTER-KEY 消息，否则发出错误消息。当密钥确定以后，服务器端将向客户端发出 SERVER-VERIFY 消息。只有拥有合适公钥的服务器才能解开密钥。第一阶段的流程如图 9-4 所示。

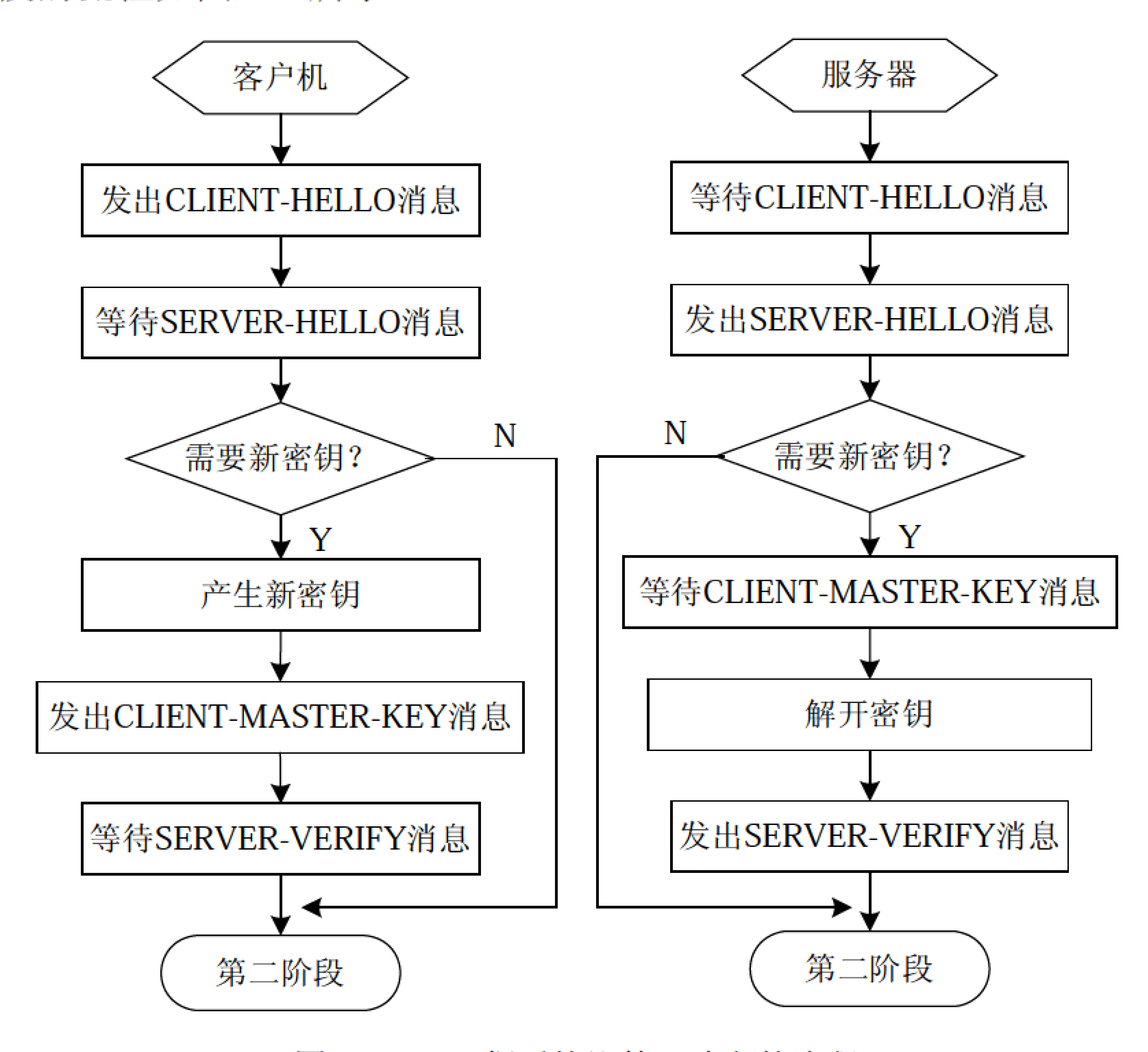
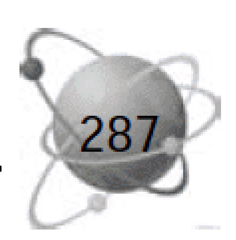


图 9-4　SSL 握手协议第一阶段的流程



需要注意的是，每一个通信方向上都需要一对密钥，所以一个连接需要 4 个密钥，分别为客户端的读密钥、客户端的写密钥、服务器端的读密钥、服务器端的写密钥。

第二阶段的主要任务是对客户端进行认证。此时服务器已经被认证了，它将向客户端发出认证请求消息 REQUEST-CERTIFICATE。当客户端收到服务器端的认证请求消息时，将发出自己的证书，并且监听对方回送的认证结果。而当服务器收到客户端的认证后，认证成功返回 SERVER-FINISH 消息，否则返回错误消息。

3）SSL 的安全功能

（1）SSL 安全概述

SSL 是一种用于 Web 的安全通信标准，可以把它理解成分层体系结构中的一层，位于应用层和传输层之间，负责建立用户与服务器之间的加密通信，确保信息传递的安全性。数据经过它流出的时候被加密，再往 TCP/IP 传送；而从 TCP/IP 流入之后，数据也要先进入这一层被解密。同时，它还能验证网络连接两端的身份。SSL 可以对各种应用数据进行加密，例如 HTTP、POP、FTP 等。SSL 提供的安全机制可以保证应用层数据在传输时不被监听、伪造和篡改。

SSL 工作在公钥和私钥基础上，任何用户都可以获得公钥来加密数据，但解密数据必须要通过相应的私钥。使用 SSL 安全机制时，首先客户端与服务器端建立连接，服务器端把它的数字证书与公钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私钥才能解密。这样，客户端和服务器端就建立了一个安全通道。

Web 客户机通过连接到一个支持 SSL 的服务器，启动一次 SSL 会话。支持 SSL 的典型 Web 服务器在一个与标准 HTTP 请求（默认为端口 80）不同的端口（默认为 443）上接受 SSL 连接请求。当客户机连接到这个端口上时，它将启动一次建立 SSL 会话的握手。当握手完成之后，通信内容被加密，并且执行消息完整性检查，从而得知 SSL 会话过期。在此期间，握手必须只发生过一次。

SSL 协议的优点是它提供了连接安全性，具有以下 3 个基本属性。

① 连接的私有性：在初始握手定义了一个会话密钥后，使用会话密钥进行加密通信。对数据的加密采用了对称加密技术，例如 DES 和 RC4 等。

② 连接的认证性：通过密码技术（例如 RSA 和 DSS）来验证对等实体的身份。

③ 连接的可靠性：消息传输使用一个带密钥的消息认证码 MAC，包括了消息完整性检查。其中，MAC 是通过把密钥和消息一起经安全哈希函数（如 SHA 和 MD5）处理后得到的。

（2）SSL 中使用的加密技术

在 SSL 中，分别采用了对称密码、公钥密码和公钥密码中的数字签名技术。公钥密码技术用于初始化 SSL 连接，对称密码技术用于 SSL 连接后的安全通信。

使用 SSL 的 Web 服务器持有私钥和带有公钥信息的证书。当 Web 浏览器请求获取 Web 服务器上的服务时，一个初始化 SSL 连接的过程便开始了。这个初始化过程如下：

① 客户端使用 HTTP 协议向 Web 服务器发出对某个页面的请求。

② Web 服务器把含有服务器公钥的证书发送给客户端。

③ 客户端进行一系列的检查，包括证书是否过期；签发此证书的安全认证中心 CA 是否存在于浏览器的可信任 CA 列表中；Web 服务器的全称域名 FQDN（Fully Qualified Domain Name）是否和证书中的 CN（Common Name）匹配。

如果各项检查都通过，SSL 连接的初始化工作就完成了，SSL 连接被建立，否则 SSL 连接失败。

提示：对于客户端的第二项检查，当 CA 不在信任列表中时也可以建立连接，只不过浏览器会提示用户这个证书来自不可信任的机构，是否继续等，这时只要选择“是”即可继续此过程。

当 SSL 连接建立后，使用对称密钥用于实际的数据传输，因为使用相同的密钥加密和解密会节省系统资源。这个密钥在 SSL 连接初始化过程中由客户端指定，并通过公钥密码技术与服务器端协商确定。

（3）证书的申请和签发

从上面的 SSL 工作过程中可以发现，对 Web 系统的加密离不开密钥对的产生和证书的签发（由 CA 负责完成证书的签发）。

公/私密钥对的产生有两种方式：一种方式是由用户在自己的机器上生成密钥对，用户向 CA 申请证书时只传递公钥，私钥自己保留，因此安全性高；另一种方式是由可信任的第三方，即 CA 机械地为客户生成密钥对。

在第一种方式中，用户在生成密钥对后，可以花钱让 CA 签署证书。这时用户要生成一个证书请求上传给 CA，其中包括密钥对的公钥部分，等待 CA 的签发。如果用户是为了测试用，可以自己建立 CA 并签发证书。

一般情况下，Web 应用中的数据经过简单的由上到下的几次封装，就进入网络，如果这些包被截获的话，那么可以很容易地根据网络协议得到里面的数据，包括登录用户名/密码等信息。用类似 Sniffer 这样的监听工具可以很容易地做到这一点。SSL 可以作为对策之一，帮助提高 Web 系统的安全性。

4）SSL 与 TLS

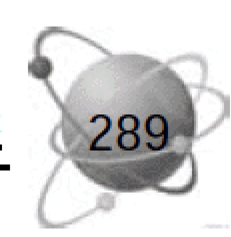
最新版本的传输层安全协议（Transport Layer Security，TLS）是 Internet 工程任务组 IETF 制定的一种新协议，建立在 SSL 3.0 协议规范之上，是 SSL 3.0 的后续版本。在 TLS 与 SSL 3.0 之间存在着明显的差别，主要是它们所支持的加密算法不同，所以 TLS 与 SSL 3.0 不能互操作。

（1）TLS 与 SSL 的差异

① 版本号：TLS 记录格式与 SSL 记录格式相同，但版本号的值不同，TLS 的版本 1.0 使用的版本号为 SSL 3.1。

② 报文鉴别码：SSL 3.0 和 TLS 的 MAC 算法及 MAC 计算的范围不同。TLS 使用了 RFC-2104 定义的 HMAC 算法，SSL 3.0 使用了相似的算法，两者的差别在于 SSL 3.0 中填充字节与密钥之间采用的是连接运算，而 HMAC 算法采用的是异或运算；但是两者的安全程度是相同的。

③ 伪随机函数：TLS 使用了称为 PRF 的伪随机函数来将密钥扩展成数据块，是更安



全的方式。

④ 报警代码：TLS 支持几乎所有的 SSL 3.0 报警代码，而且 TLS 还补充定义了很多报警代码，例如解密失败、记录溢出、未知 CA、拒绝访问等。

⑤ 密文族和客户证书：SSL 3.0 和 TLS 存在少量差别，即 TLS 不支持 Fortezza 密钥交换、加密算法和客户证书。

⑥ CERTIFICATE VERIFY 和 FINISHED 消息：SSL 3.0 和 TLS 在用 CERTIFICATE VERIFY 和 FINISHED 消息计算 MD5 和 SHA-1 散列码时，计算的输入有少许差别，但安全性相当。

⑦ 加密计算：TLS 与 SSL 3.0 在计算主密值（Master Secret）时采用的方式不同。

⑧ 填充：用户数据加密之前，需要增加的填充字节不同。在 SSL 中，填充后的数据长度要达到密文块长度的最小整数倍；而在 TLS 中，填充后的数据长度可以是密文块长度的任意整数倍（但填充的最大长度为 255 字节），这种方式可以防止基于对报文长度进行分析的攻击。

（2）TLS 的主要增强内容

TLS 的主要目标是使 SSL 更安全，并使协议的规范更精确和完善。TLS 在 SSL 3.0 的基础上，提供了以下增强内容。

① 更安全的 MAC 算法。

② 更严密的警报。

③“灰色区域”规范的更明确定义。

（3）TLS 对于安全性的改进

① 对于消息认证使用密钥散列法：TLS 使用消息认证代码的密钥散列法 HMAC，当记录在开放的网络（例如因特网）上传送时，该代码确保记录不会被变更。SSL 3.0 提供了键控消息认证，但 HMAC 比 SSL 3.0 使用的消息认证代码 MAC 功能更安全。

② 增强的伪随机功能 PRF：PRF 生成密钥数据。在 TLS 中，HMAC 定义 PRF。PRF 使用两种散列算法保证其安全性，如果任一算法暴露了，只要第二种算法未暴露，则数据仍然是安全的。

③ 改进的已完成消息验证：TLS 和 SSL 3.0 都对两个端点提供已完成的消息，该消息认证交换的信息没有被变更。然而，TLS 将此已完成消息基于 PRF 和 HMAC 值之上，这也比 SSL 3.0 更安全。

④ 一致证书处理：与 SSL 3.0 不同，TLS 试图指定必须在 TLS 之间实现交换的证书类型。

⑤ 特定警报消息：TLS 提供更多的特定和附加警报，以指示任一会话端点检测到的问题；同时还对何时应该发送某些警报进行记录。

2. 安全电子交易协议 SET

电子商务的一个主要特征是在线支付，即以 Internet 为通信手段，以金融电子化网络为基础，以各类交易卡为媒介，以电子数据形式存储在银行的计算机系统中，通过计算机网络系统以电子信息的传递形式，实现交易双方的资金转账和付款。

为了保证在线支付的安全，需要采用数据加密和安全认证技术，以便营造一个可信赖的电子交易环境。尽管公开密钥加密、数字签名、电子信封、数字证书等保证系统安全的技术手段已经存在，但安全问题是系统性的问题，并非把这些手段简单地结合在一起就可得到安全。电子支付系统目前尚处于不成熟阶段且种类较多，比较而言，SET 协议是一个较完善的通过 Internet 进行安全资金支付的技术标准。

安全电子交易协议（Secure Electronic Transaction，SET）是一个通过开放网络（包括 Internet）进行安全资金支付的技术标准，由万事达（MasterCard）国际组织和维萨（Visa）国际组织在微软公司、网景公司、IBM 公司、GTE 公司、SAIC 及其他公司的支持下联合设计的安全协议。起初，MasterCard、网景公司和 IBM 一起开发了一种基于加密套接字协议层 SSL 的交易安全系统，称为安全加密结算协议 SEPP；而它们各自的对手 Visa 和微软则开发了另一种标准安全交易技术 STT 作为反击。来自银行业的压力最终迫使这两方开展合作，开发出了安全电子交易 SET 作为共同遵守的标准。

SET 本身不是一个支付系统，而是一个安全协议和格式的集合，使得用户可以以一种安全的方式，将已经存在的信用卡支付基础设施配置在开放网络上，例如 Internet。

SET 的目的是为通过互联网在网站和处理银行之间传输结算卡结算信息时提供安全保障。虽然安全套接层 SSL 协议保证了在商家和消费者之间传输数据和其他敏感信息的安全，但它不能验证消费者是否是结算卡的持有人。SET 标准的安全程度很高，它结合了数据加密标准 DES、RSA 算法、加密套接字协议层 SSL 和安全超文本传输协议 S-HTTP，为每一项交易都提供了多层加密。SET 自 1997 年 5 月由 MasterCard 和 Visa 两大信用卡组织联合推出以来，由于它得到了 IBM、HP、Microsoft、Netscape、VeriFone、GTE、Terisa 和 VeriSign 等很多大公司的支持，已成为事实上的工业标准，目前已获得 IETF 标准的认可。

（1）SET 的体系结构

电子商务的工作流程与实际的购物流程非常接近，从顾客通过浏览器进入在线商店开始，一直到所订购的物品送货上门或所订的服务完成，以及账户上的资金转移，所有这些都是通过公用网络 Internet 完成的。如何保证网上传输数据的安全和交易双方的身份确认是电子商务能否得到推广的关键，也正是 SET 所要解决的最主要问题。下面就是一种基于 SET 协议的电子商务系统的体系结构，如图 9-5 所示。

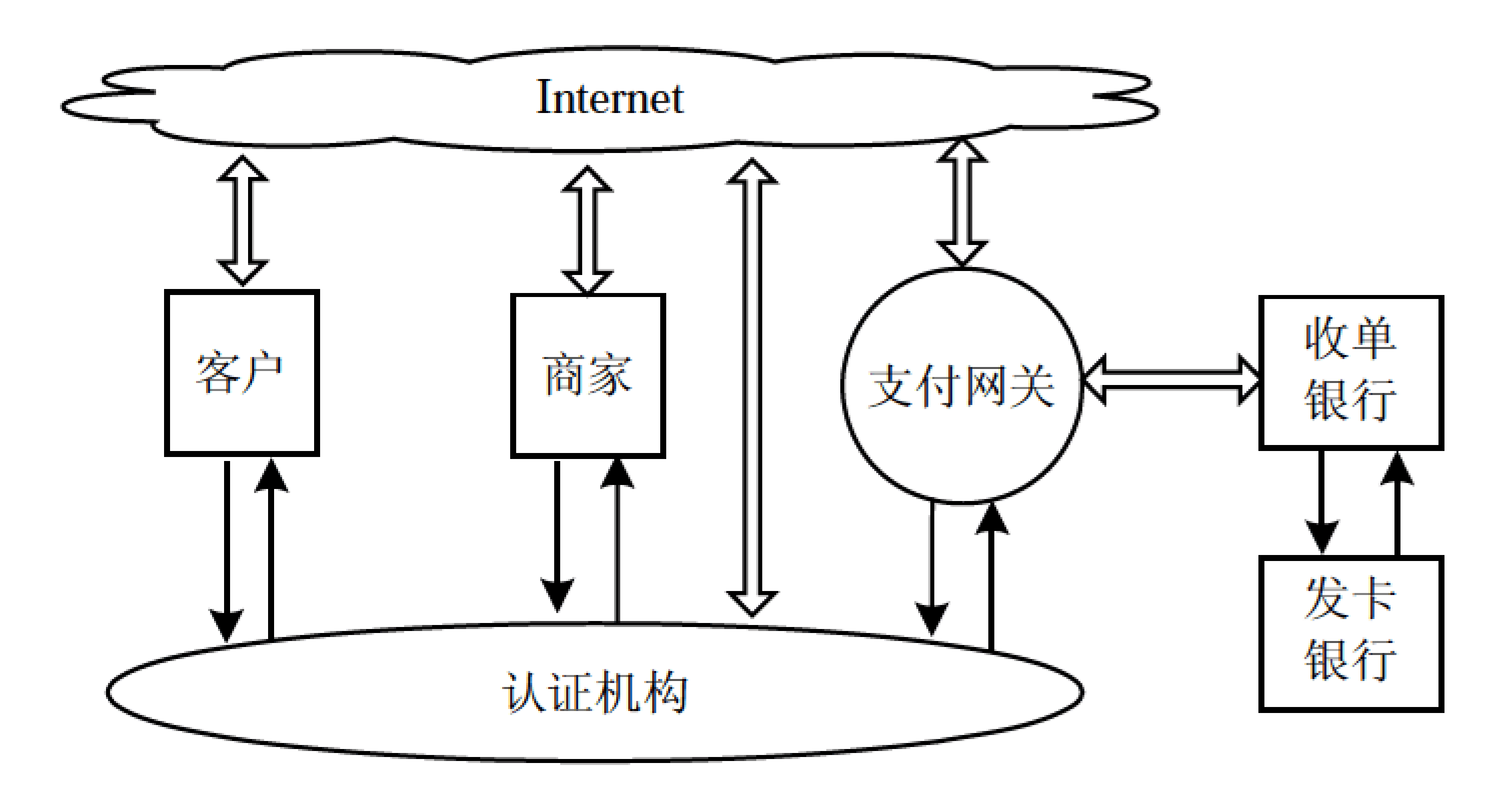
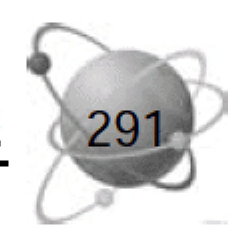


图 9-5　一种基于 SET 协议的电子商务系统的体系结构



一个完整的 SET 处理流程中的各个参与者如下：

- 消费者：包括个人消费者和团体消费者，按照在线商店的要求填写定货单，通过由发卡银行发行的信用卡进行付款。
- 商家：提供商品或服务，具备相应电子货币使用的条件。
- 收单银行：通过支付网关处理消费者和在线商店之间的交易付款问题。
- 发卡银行：电子货币（例如智能卡、电子现金、信用卡）的发行公司，以及某些兼有电子货币发行的银行，负责处理电子货币的审核和支付工作。
- 支付网关：银行金融系统与因特网之间的接口，可以将因特网上的传输数据转换成金融机构内部的数据。
- 认证机构 CA：负责对交易双方的身份确认，对厂商的信誉度和消费者的支付手段进行认证。CA 在整个电子商务过程中至关重要，是开展电子商务的基础。CA 具有证书发放、证书更新、证书撤销和证书验证功能。CA 证书可分为：持卡人证书、商家证书、支付网关证书、银行证书、发卡机构证书。它通常是企业性服务机构，受理数字证书的申请、签发及管理。

（2）基于 SET 的支付流程

下面是一个完整的基于 SET 的支付流程，如图 9-6 所示。

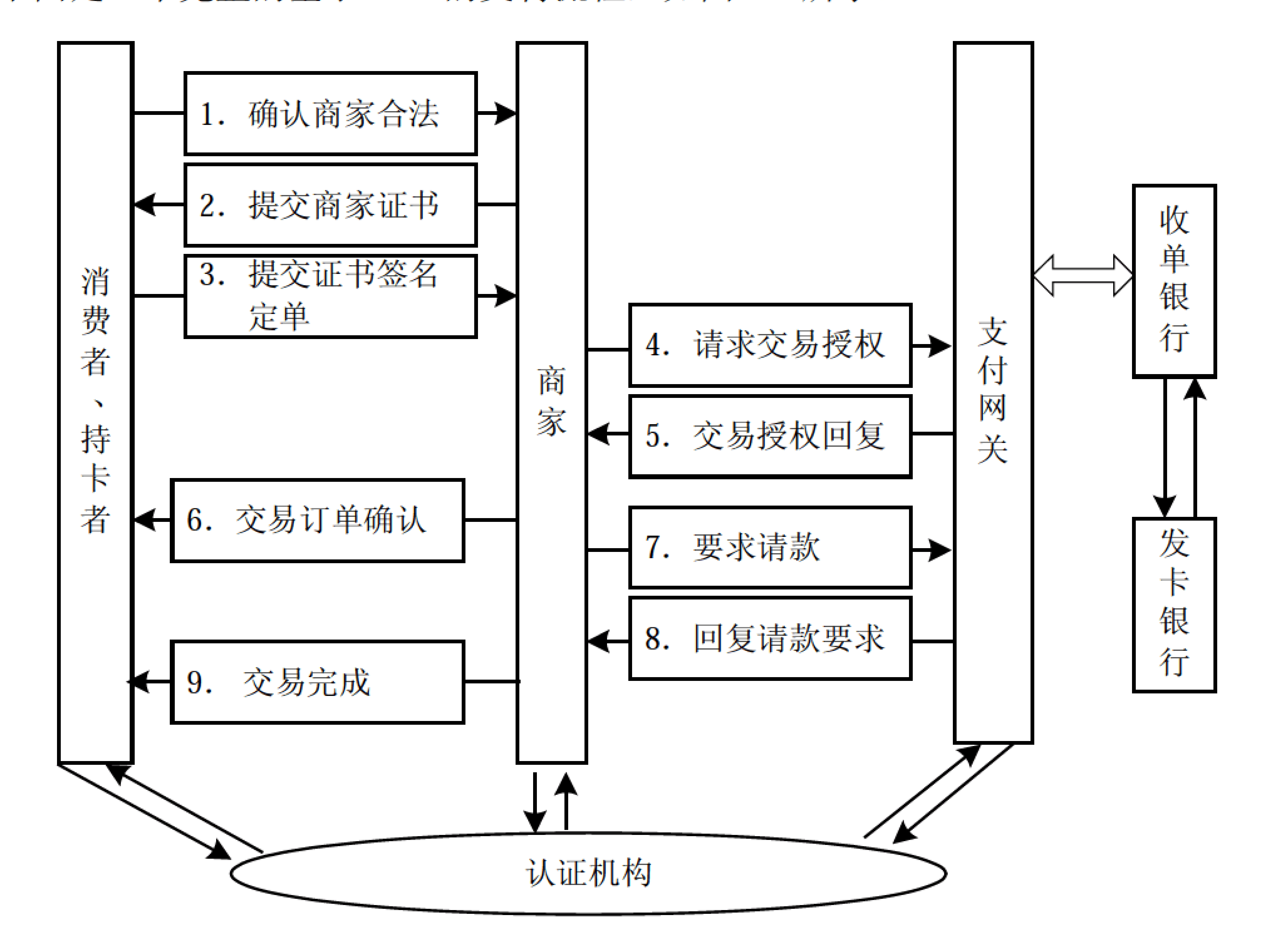


图 9-6 一个完整的基于 SET 的支付流程

① 持卡者向商家发出购买初始化请求，包含持卡者的信息和数字证书。

② 商家接收到请求后，通过 CA 验证持卡者的身份，将商家和支付网关的有关信息和证书生成回复消息，发给持卡者。

③ 持卡者接收到消息后，通过 CA 验证商家和支付网关的身份；然后，持卡者利用自己的支付信息（包括账户信息）生成购买请求消息，并发送给商家。

其中，持卡者利用加密技术，使得商家只能读购买信息，支付网关只能读账户信息。

④ 商家接收到后，通过解密读到购买信息，连同自己的信息及持卡人信息，一同加密生成授权请求消息，发给支付网关，请求支付网关授权该交易。

⑤ 支付网关接收到后，解密取出支付信息，通过银行内部网络连接收单银行和发卡银行，对该交易进行授权。授权完成后，支付网关产生授权响应消息，发给商家。

⑥ 商家接收到后，定期向支付网关发出转账请求消息，请求进行转账。

⑦ 支付网关接收到后，通过银行内部网络连接收单银行和发卡银行，将资金从持卡者账户转到商家账户中，然后向商家发出消息。

⑧ 商家接收到消息后，知道已经完成转账，然后产生消息，发送给持卡者。

⑨ 持卡者接收到消息，知道该交易已经完成。

SET 协议通过数字证书、CA 以及 CA 的树形验证体系结构完成认证过程。

（3）基于 SET 协议的电子支付分析

SET 是一个多方的消息报文协议，定义了银行、商家、持卡者之间必需的报文规范，利用公开密钥加密、数字签名、数字证书等技术，解决了电子商务交易中消费者、商家、银行之间的在线支付，保证了交易的机密性、信息完整性、身份真实性及不可否认性，保护了参与各方的利益。

① 机密性

SET 协议采用先进的公开密钥算法来保证传输信息的机密性，以避免 Internet 上任何无关方的窥探。公开密钥算法容许任何人使用公钥将加密信息发送给指定的接收者，接收者收到密文后，用私钥对该信息解密，因此只有指定的接收者才能读取该信息，从而保证信息的机密性。

SET 协议也可通过双重签名的方法将信用卡信息直接从客户方通过商家发送到商家的开户行，而不容许商家访问客户的账号信息，这样客户在消费时可以确信其信用卡号没有在传输过程中被窥探，而接收 SET 交易的商家因为没有访问信用卡信息，故免去了在其数据库中保存信用卡号的责任。

② 数据完整性

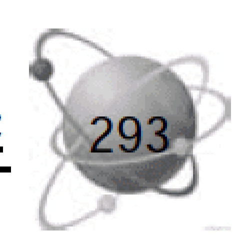
通过 SET 协议发送的所有报文加密后，将为之产生一个唯一的报文摘要值，一旦有人企图篡改报文中包含的数据，该摘要值就会改变，从而被检测到，这就保证了信息的完整性。

③ 身份验证

SET 协议可使用各方共同信任的 CA 发放的数字证书来确认交易涉及的各方（包括商家、持卡客户、授卡行和支付网关）的身份，为在线交易提供一个完整的可信赖的环境。

④ 不可否认性

SET 交易中数字证书的发布过程也包含了商家和客户在交易中存在的信息。因此，如果客户用 SET 发出一个商品的订单，在收到货物后即不能否认发出过这个订单；商家以后



也不能否认接到过这个订单。

对于商家而言，SET 利用 RSA 及数字证书保证了持卡人的合法性和不可否认性，为商家提供保护手段，使得商家免受欺诈的困扰；对于消费者而言，SET 保证了商家不会窃取用户的信用卡号，支付网关不会得到用户的购买请求，为消费者保守了更多的秘密，从而使消费者在线购物时更加轻松；对于银行和发卡机构以及各种信用卡组织，SET 帮助它们将业务扩展到 Internet 这个广阔的空间，从而减少信用卡网上支付的欺骗概率，这使得它比其他的支付方式具有更大的竞争优势。SET 协议比较完善和严谨，但是比较复杂，开发和使用比较麻烦，造成运行速度较慢。

电子支付的安全问题是电子商务发展过程中的关键问题。SET 协议位于应用层，规范了整个电子商务的活动流程，能够在银行内部网络或者其他网络上传输，允许各方之间的报文交换不是实时的，从信用卡持卡者到商家、支付网关、认证中心及信用卡结算中心，对其间的信息流向及各方必须参与的加密和认证都制定了严格的标准，从而最大限度地保证了电子支付交易的身份真实性、传输安全性、信息完整性及不可否认性。

9.3.4　电子商务系统安全案例

由于 Windows NT 系统的易维护性，越来越多的中小企业在自己的网站上和内部办公管理系统上采用它，而且很多都是用默认的 IIS 来做 Web 服务器使用。但威胁 Windows NT 系统的有些漏洞是由于 IIS 配置不当造成的，而且可以预见，未来 IIS 还会被发现更多新的漏洞和安全问题，但只要我们做好合理的安全配置，还是可以避免很多安全隐患的。下面就是通过 SSL 加密 HTTP 通道来加强 IIS 安全，从而增强 Web 电子商务系统安全的一个实例。

1. 建立 SSL 安全机制

IIS 的身份认证除了匿名访问、基本验证和 Windows NT 请求/响应方式外，还有一种安全性更高的认证，就是通过 SSL 安全机制使用数字证书。SSL 位于 HTTP 层和 TCP 层之间，用于建立用户与服务器之间的加密通信，确保所传递信息的安全性。SSL 是工作在公钥和私钥基础上的，任何用户都可以获得公钥来加密数据，但解密数据必须要通过相应的私钥。使用 SSL 安全机制时，首先客户端与服务器建立连接，服务器把它的数字证书与公钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私钥才能解密，这样客户端和服务器端就建立了一条唯一的安全通道。

建立了 SSL 安全机制后，只有 SSL 允许的客户才能与 SSL 允许的 Web 站点进行通信，并且在使用统一资源定位符 URL 时，输入“https://”，而不是“http://”。

简单地说，默认情况下我们所使用的 HTTP 协议是没有任何加密措施的，所有的消息全部都是以明文形式在网络上传送的，恶意的攻击者可以通过安装监听程序来获得我们和服务器之间的通信内容。所以，全面加密整个网络传输通道的确是个很好的安全措施。

2. 为 Web 服务器配置 SSL

要在 IIS 中启用 SSL，首先必须获得用于加密和解密通过网络传输的信息的证书。IIS 具有自己的证书请求工具，此工具简化了获取证书的过程，可以更便捷地向证书颁发机构发送证书请求。

在 IIS 中，收到来自证书颁发机构的证书文件后，必须将其配置在计算机上。在 IIS 中，通过网站或文件夹属性的“目录安全性”选项卡来配置和管理证书。

3. 配置文件夹或网站以使用 SSL/HTTPS

此过程假定用户的站点已经具备了证书。

（1）以管理员身份登录到 Web 服务器。

（2）单击“开始”，指向“设置”，然后单击“控制面板”。

（3）双击“管理工具”，然后双击“Internet 服务管理器”。

（4）从左窗格中的不同服务站点列表中选择网站。

（5）右击希望为其配置 SSL 通信的网站、文件夹或文件，然后单击“属性”。

（6）选择“目录安全性”选项卡。

（7）单击“编辑”。

（8）如果希望网站、文件夹或文件要求 SSL 通信，单击“需要安全通道（SSL)”。

（9）单击“需要 128 位加密”，以配置 128 位（而不是 40 位）加密支持。

（10）要允许用户不必提供证书就可以连接，则单击“忽略客户证书”；如果要让用户提供证书，则使用“接受客户证书”。

（11）要配置客户端映射，则单击“启用客户证书映射”，然后单击“编辑”将客户证书映射到用户。如果配置了此功能，可以将客户证书分别映射到活动目录中的每个用户。可以使用此功能以根据用户访问网站时提供的证书自动识别用户。可以将用户一对一映射到证书（一个证书标识一个用户），或者将许多证书映射到一个用户（根据特定的规则，对照证书列表来匹配特定的用户。第一个有效的匹配项称为映射）。

（12）单击“确定”。

9.4 黑客与网络攻击

随着网络的迅猛发展，网络安全问题日趋严重，黑客攻击活动日益猖獗，黑客攻击的预防技术成为当今社会关注的焦点，可以说目前网络安全防护的主要课题便是如何预防和阻止黑客攻击。

9.4.1 概述

“黑客”的英文是 Hacker，原意是“开辟、开创”之意，也就是说“黑客”应该是开

辟道路的人。

现在的黑客组织主要分成两大阵营，通常称做“白帽”和“黑帽”。

“白帽”黑客代表那些热衷于学习和使用电脑系统，且对某些课题有着极为深入研究的人。他们对商业、网络防护等领域较有兴趣，热爱挑战，通常只是单纯因为好玩而以合法的方式运用其黑客攻击技术。典型的例子有参与渗透测试，开发并运用防护和攻击消减工具，或受聘为安全管理人员和安全顾问。实际上，在计算机世界里，“黑客”这个词最早就是用来描述此类人。

“黑帽”黑客则是对“黑客”这个词更惯常的理解。正如电影或媒体所描述的，作为蓄意破坏者和强迫型的社会边缘人，黑客总是在寻求制造混乱，摧毁一切美好的事物，他们对网络进行恶意扫描、攻击和渗透，应用专门技术找到并利用系统的不安全因素来进行破坏。

现实中，这两个阵营之间还有一块灰色地带，即并不是所有的“白帽”黑客的行为都是合法的，同样“黑帽”黑客的行为也并不全是非法的。这就可以解释为什么很多原先的“黑帽”后来变成了“白帽”。这完全取决于其动机驱动因素，这些因素的根蒂在于好奇心、窃取信息、挑战智力、无政治主义及赢利等思想观念。

9.4.2　网络攻击的类型

目前的网络攻击模式呈现多方位、多手段化，让人防不胜防。概括来说，网络攻击可以分为 4 大类，即拒绝服务攻击、利用型攻击、信息收集型攻击、假消息攻击。

1. 拒绝服务攻击

拒绝服务（Denial of Service，DoS）攻击是目前最常见的一种攻击类型。从网络攻击所采用的各种方法和所产生的破坏情况来看，DoS 算是一种很简单，但又很有效的进攻方式，也是最容易实施的攻击行为。其目的就是拒绝服务访问，破坏组织的正常运行，最终使网络连接堵塞，或者服务器因疲于处理攻击者发送的数据包而使服务器系统的相关服务崩溃、系统资源耗尽。

DoS 的攻击方式有很多种，常见的 DoS 攻击方式有同步洪流（SYNFlood）、死亡之 Ping（Ping of Death）、Finger 炸弹、Land 攻击、Ping 洪流、Rwhod 和 Smurf 等。

DoS 攻击的基本过程如下：首先攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复消息后等待回传消息。由于地址是伪造的，所以服务器一直等不到回传的消息，然而服务器中分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

这类攻击和其他大部分攻击不同的是，它们不是以获得网络或网络上信息的访问权为目的，而是要使受攻击方耗尽网络、操作系统或应用程序有限的资源而崩溃，从而不能为其他正常用户提供服务。这就是这类攻击被称为“拒绝服务攻击”的真正原因。

若涉及特殊的网络服务应用，像 HTTP 或 FTP 服务，攻击者能够获得并保持所有服务

器支持的有用连接，有效地把服务器或服务的真正使用者拒绝在外面。大部分拒绝服务攻击是利用被攻击系统整体结构上的弱点，而不是利用软件的小缺陷或安全漏洞进行的。然而，有些攻击通过采用无用的网络报文掀起网络风暴，提供错误的网络资源状态信息危及网络的性能。

分布式拒绝服务（Distributed Denial of Service，DDoS）是一种基于 DoS 的特殊形式的分布、协作式的大规模拒绝服务攻击。也就是说，不再是从单一的地点攻击，而是同时在几个，甚至十几个地点实施拒绝服务攻击。由此可见，它的攻击力度更大，危害性当然也就更大了。它主要瞄准比较大的网站，像商业公司、搜索引擎和政府部门的 Web 站点。

2. 利用型攻击

利用型攻击是一类试图直接对用户的机器进行控制的攻击，最常见的有 3 种：口令猜测、特洛伊木马和缓冲区溢出。

（1）口令猜测

一旦黑客识别了一台主机而且发现了基于 NetBIOS、Telnet 或 NFS 等服务的可利用的用户账号，通过成功的口令猜测即令达到对机器的控制。建议用户选用难以猜测的口令，例如词和标点符号的组合；确保像 NFS、NetBIOS 和 Telnet 这样可利用的服务不暴露在公共范围内，如果该服务支持锁定策略，就进行锁定，这样可以较好地防御口令猜测。

（2）特洛伊木马

“特洛伊木马”是一种或是直接由一个黑客，或是通过一个不令人起疑的用户秘密安装到目标系统的程序。一旦安装成功并取得管理员权限，安装此程序的人就可以直接远程控制目标系统。“特洛伊木马”程序可用来查找密码信息，留下后门使得黑客日后可以再次进入系统。“特洛伊木马”程序与病毒类似，但是它不进行自我复制，而是驻留在计算机内部进行破坏或允许其他人对此电脑进行远程控制。

实际上，通常黑客使用“特洛伊木马”进行秘密的间谍活动（例如包嗅探）或通过后门功能来实现对被渗透电脑的远程控制，而电脑用户却对此毫不知情。“特洛伊木马”可能造成的破坏结果包括删除/覆盖数据；毁坏文档；传播病毒等其他恶性产物；建立受感染计算机网络，来发动分布式拒绝服务（DDoS）攻击或发送垃圾邮件；监控电脑使用者并暗地里将其上网习惯等数据报告给其他人；记忆键盘操作，盗取用户的密码、信用卡号等私人信息；使用网络钓鱼的伎俩诈骗用户资料用于犯罪活动；在电脑中安装后门程序，便于日后再次访问控制。

（3）缓冲区溢出

通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，即可破坏程序的堆栈，使程序转而执行其他的指令。如果这些指令是放在有 Root 权限的内存中，那么一旦这些指令得到了运行，黑客就能够以 Root 权限控制系统，达到入侵的目的。缓冲区攻击的目的在于扰乱某些以特权身份运行的程序的功能，使攻击者获得程序的控制权。

缓冲区溢出的一般攻击步骤为：在程序的地址空间里安排适当的代码，再通过适当的地址初始化寄存器和存储器，让程序跳到黑客安排的地址空间中执行。

缓冲区溢出给系统带来了巨大的危害，要有效地防止这种攻击，应该做到以下几点。

① 必须及时发现缓冲区溢出这类漏洞：在一个系统中（如 UNIX 操作系统），这类漏洞是非常多的，系统管理员应经常和系统供应商联系，及时对系统升级以堵塞缓冲区溢出漏洞。

② 程序指针完整性检查：在程序指针被引用之前检测它是否改变。即便一个攻击者成功地改变了程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不会被使用。

③ 堆栈保护：这是一种提供程序指针完整性检查的编译器技术，通过检查函数活动记录中的返回地址来实现。在堆栈中，函数返回地址后面加了一些附加的字节，而在函数返回时，首先检查这个附加的字节是否被改动过。如果发生过缓冲区溢出攻击，那么这种攻击很容易在函数返回前被检测到。但是，如果攻击者预见到这些附加字节的存在，并且能在溢出过程中同样地制造它们，那么它就能成功地跳过堆栈保护的检测。

④ 数组边界检查：所有对数组的读/写操作都应当检查，以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作，通常可以采用一些优化的技术来减少检查的次数。

3. 信息收集型攻击

信息收集型攻击并不对目标本身造成危害，主要被用来为进一步入侵提供有用的信息，主要包括扫描技术、体系结构探测、利用信息服务。

（1）扫描技术

网络安全扫描技术是一种基于 Internet 远程检测目标网络或本地主机安全性脆弱点的技术。通过网络安全扫描，系统管理员能够发现所维护的 Web 服务器的各种 TCP/IP 端口的分配、开放的服务、Web 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞。网络安全扫描技术也是采用积极的、非破坏性的方法来检验系统是否有可能被攻击。它利用了一系列的脚本模拟对系统进行攻击的行为，并对结果进行分析。这种技术通常被用来进行模拟攻击实验和安全审计。网络安全扫描技术与防火墙、安全监控系统互相配合就能够为网络提供很高的安全性。当然，网络扫描技术也可以被黑客利用，成为黑客收集信息的工具和手段。

网络扫描技术主要包括 PING 扫射（Ping Sweep）、操作系统探测（Operating System Identification）、探测访问控制规则（Firewalking）、端口扫描（Port Scan）以及漏洞扫描（Vulnerability Scan）等。

（2）体系结构探测

黑客使用具有已知响应类型数据库的自动工具，对来自目标主机的、对坏数据包传送所作出的响应进行检查。由于每种操作系统都有其独特的响应方法（例如 NT 和 Solaris 的 TCP/IP 堆栈具体实现就有所不同），通过将此独特的响应与数据库中的已知响应进行对比，黑客就能确定出目标主机所运行的操作系统。

（3）利用信息服务

利用信息服务主要利用网络协议上存在的漏洞或者网络服务存在的缺陷进行网络攻

击。主要有以下几类：

① DNS 域转换：DNS 协议不对转换或信息的更新进行身份认证，这使得该协议被人以一些不同的方式加以利用。如果用户维护着一台公共的 DNS 服务器，黑客只需实施一次域转换操作就能得到服务器中所有主机的名称以及内部 IP 地址。

② Finger 服务：使用 Finger 命令来刺探一台 Finger 服务器，就可以获取关于该系统的用户信息，从而有针对性地实施攻击。

③ LDAP 服务：通过 LDAP 协议窥探网络内部的系统及其用户信息。

4. 假消息攻击

假消息攻击主要针对目标配置不正确的消息，主要包括 DNS 高速缓存污染、伪造电子邮件。

（1）DNS 高速缓存污染：由于 DNS 服务器与其他名称服务器交换信息的时候并不进行身份验证，这就使得黑客可以将不正确的信息掺进来并把用户引向黑客自己的主机。一般来说，在防火墙上过滤入站的 DNS 更新，使外部 DNS 服务器不能更改内部服务器对内部机器的认识，就可以防范 DNS 高速缓存污染。

（2）伪造电子邮件：由于 SMTP 并不对邮件发送者的身份进行鉴定，因此黑客可以对内部客户伪造电子邮件，声称是来自某个客户认识并相信的人，并附带上可安装的“特洛伊木马”程序，或者是一个引向恶意网站的链接。可以使用 PGP 等安全工具，并安装电子邮件证书来防范伪造电子邮件。

9.4.3 黑客攻击流程

黑客要实施攻击，一般来说必须有 3 个基本步骤。

（1）收集信息（踩点）。

（2）选择目标，实施攻击。

（3）上传黑客程序，取得控制权，下载用户数据。

黑客攻击的关键一步就是收集信息，也就是踩点。在攻击者对特定的网络资源进行攻击前，他们需要了解将要攻击目标的环境，这需要收集汇总各种与目标系统相关的信息，包括目标网络结构、用户数、目标机器类型、所用域，以及 IP 地址和操作系统等。

攻击者收集目标信息也不是一步到位的，也必须经过一系列的子步骤来实现。首先，黑客要做的工作一般是扫描，随机地或者是有针对性地利用扫描器去发现目标网络上那些有漏洞的机器，像程序的溢出漏洞、CGI、Unicode、FTP、数据库漏洞等，都是黑客希望看到的扫描结果。随后就是尝试入侵了。

黑客入侵的一般模式为：踩点→查点→扫描→分析并入侵→获取权限→提升权限→扩大范围→安装后门→清除日志。黑客攻击行为流程的一般模型如图 9-7 所示。

图 9-7 中虚线框上部完成收集信息；虚线框中是入侵模块，即实施攻击；最后完成黑客攻击的目的。

踩点
得到用户E-mail
得到域名或IP地址
入侵行为模块
扫描
得到端口
系统账号表
网络信息资源
发送恶意邮件
DoS攻击
攻击网络服务
远程口令猜解
获取网络资源
系统崩溃
获取访问权
其他手段
提升权限
导入LC本地破解
获取控制权
安装后门
安装跳板
安装Sniffer
资源扩张
清除/伪造痕迹
获取sam密码散列
远程控制
转移目标
获得sam信息
直接在局域网嗅探
嗅探
获得账号口令
获得控制权

图 9-7　黑客攻击行为流程的一般模型

9.4.4　典型网络攻击及防范措施举例

1. TCP SYN 洪水（TCP SYN Flood）攻击

TCP/IP 栈只能等待有限数量的应答 ACK 消息，因为每台计算机用于创建 TCP/IP 连接的内存缓冲区都是非常有限的。如果这一缓冲区充满了等待响应的初始信息，则该计算机就会对接下来的连接停止响应，直到缓冲区里的连接超时。

"TCP SYN 洪水"攻击正是利用了这一系统漏洞来实施攻击的。攻击者利用伪造的 IP 地址向目标发出多个连接 SYN 请求。目标系统在接收到请求后发送确认信息，并等待回答。由于黑客们发送请求的 IP 地址是伪造的，所以确认信息不会到达任何计算机，当然也就不会有任何计算机为此确认信息作出应答了。而在没有接收到应答之前，目标计算机系统是不会主动放弃的，会继续在缓冲区中保持相应连接信息，一直等待。当等待连接达到一定数量后，缓冲区资源耗尽，从而开始拒绝接收任何其他连接请求，当然也包括本来属于正常应用的请求，这就是黑客们的最终目的。

防御方法：可以通过检查单位时间内收到的SYN连接是否超过系统设定的值来检测是否存在这种攻击。反攻击的方法是当接收到大量的SYN数据包时，通知防火墙阻断连接请求或丢弃这些数据包，并进行系统审计；在防火墙上过滤来自同一主机的后续连接。不过"TCP SYN洪水"攻击还是非常令人担忧的，由于此类攻击并不寻求响应，所以无法从一个简单的高容量的传输中鉴别出来。我们也可以利用防火墙抵御"TCP SYN洪水"攻击。

2. 分片IP报文攻击

IP分组是在网络上传输IP报文时常采用的一种技术手段，但是其中存在一些安全隐患。最近，一些IP分组攻击除了用于进行拒绝服务攻击之外，还经常用于躲避防火墙或者网络入侵检测系统。部分路由器或者基于网络的入侵检测系统NIDS，由于IP分组重组能力的欠缺，导致无法进行正常的过滤或者检测。

为了传送一个大的IP报文，IP协议栈需要根据链路接口的MTU对该IP报文进行分组，通过填充适当的IP头中的分组指示字段，接收计算机可以很容易地把这些IP分组报文组装起来。目标计算机在处理这些分组报文的时候，会把先到的分组报文缓存起来，然后一直等待后续的分组报文。这个过程会消耗掉一部分内存，以及一些IP协议栈的数据结构。如果攻击者给目标计算机只发送一片分组报文，而不发送所有的分组报文，被攻击计算机便会一直等待（直到一个内部计时器到时）；如果攻击者发送了大量的分组报文，则会消耗掉目标计算机的资源，而导致不能处理正常的IP报文，这也是一种DoS攻击。

防御方法：对于这种攻击，目前还没有一种十分有效的防御方法。对一些包过滤设备或者入侵检测系统来说，首先是通过判断目的端口号来采取允许/禁止措施。但是由于某些攻击者通过恶意分组使目的端口号位于第二个分组中，而包过滤设备是通过判断第一个分组来决定后续的分组是否允许通过，因而这些分组在目标主机上进行重组之后将形成各种攻击。通过这种方法可以迂回一些入侵检测系统及一些安全过滤系统。当然，目前一些智能的包过滤设备可直接丢掉报头中未包含端口信息的分组，这样可以起到很好的防御作用。

3. netbus木马

netbus木马的客户端有两种，开放的都是12345端口，一种以Mring.exe为代表（472576字节），一种以SysEdit.exe为代表（494592字节）。

一旦运行Mring.exe，Mring.exe就会通知Windows每次启动时就运行它。Windows将它放在了注册表中，可以打开C:\Windows\Regedit.exe，进入HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run找到Mring.exe，然后删除这个键值，再到Windows中找到Mring.exe删除。值得注意的是，Mring.exe可能会被黑客改变名字，字节长度也被改变了，但是在注册表中的位置不会改变，用户可以到注册表的这个位置去找。

另外，可以查找含有netbus字符的可执行文件，再看字节的长度，被找到的文件多半就是Mring.exe的变种。

SysEdit.exe被运行以后，并不加到Windows的注册表中，也不会自动挂到其他程序中，于是有人认为这是傻瓜木马，其实这才是最可恶、最阴险的木马。别的木马被加到了注册

表中，就有痕迹可查了，而 SysEdit.exe 是挂在其他的软件中，只要不碰这个软件，SysEdit.exe 也就不会发作，可一旦运行了捆绑了 SysEdit.exe 的程序，SysEdit.exe 即会同时启动。可以在自己的计算机中做这样一个实验，将 SysEdit.exe 和 C:\Windows\System\Abcwin.exe 捆绑起来（Abcwin.exe 是智能 ABC 输入法），然后开启计算机，此时即会发现只要没有打开智能 ABC 输入法打字，SysEdit.exe 也就不会被运行，攻击者就不能进入用户计算机的 12345 端口；可一旦启动了智能 ABC 输入法（Abcwin.exe），那么捆绑在 Abcwin.exe 上的 SysEdit.exe 即会同时被运行，12345 端口被打开，也就给了攻击者以可乘之机。同样道理，SysEdit.exe 可以被捆绑到网络传呼机、信箱工具等网络工具上，甚至可以捆绑到拨号工具上，计算机中动辄数百个程序，用户怎么会知道能在什么地方发现它呢？所以说这是最最阴险的木马，让人防不胜防。

9.4.5　系统入侵后的恢复

这里主要介绍一般情况下系统如果被侵入，应该如何应对。需要注意的是，用户在系统恢复过程中的所有步骤都应该与所在组织的网络安全策略相符。

1．准备工作

（1）商讨安全策略

如果用户的组织没有自己的安全策略，那么需要按照以下过程建立自己的安全策略。

① 和管理人员协商：将入侵事件通知管理人员，这可能在有的组织中很重要。在决定进行事故恢复的时候，网络管理人员就能够得到内部各部门的配合。

② 和法律顾问协商：在开始恢复工作之前，用户的组织需要决定是否进行法律调查。

如果想找出入侵者是谁，建议你与管理人员协商并咨询法律顾问，看看入侵者是否触犯了相应的法律、法规。根据这些，可以报案，看看警方是否愿意对此进行调查。

通常，如果想进行任何类型的调查或者起诉入侵者，最好先跟管理人员和法律顾问商量，然后通知有关执法机构。需要注意的是，除非执法部门的参与，否则对入侵者进行的一切跟踪都可能是非法的。

（2）记录恢复过程中所有的步骤

记录恢复过程中采取的每一步措施是非常重要的。恢复一个被入侵的系统是一件很麻烦的事，要耗费大量的时间，因此经常会使人作出一些草率的决定。记录所做的每一步可以帮助用户避免作出草率的决定，还可以留作以后的参考，为法律调查提供帮助。

2．夺回对系统的控制权

（1）将被入侵的系统从网络上断开：为了夺回对被入侵系统的控制权，用户需要将其从网络上断开，包括拨号连接。断开以后，进入 UNIX 系统的单用户模式或者 NT 的本地管理者（Local Administrator）模式，以夺回系统控制权。

（2）复制一份被入侵系统的镜像：在进行入侵分析之前，建议备份被入侵的系统，将来可能会用得着。可以使用操作系统的相关命令完成精确复制，也可以使用一些第三方的

程序复制被入侵系统的整个硬盘镜像。建立一个备份非常重要，能帮助将系统恢复到入侵刚被发现时的状态，也可以为法律调查提供可能的帮助。

3. 入侵分析

通过审查日志文件和系统配置文件，可以检查入侵的蛛丝马迹。主要完成以下几个方面的分析：

（1）检查入侵者对系统软件和配置文件的修改

在检查入侵者对系统软件和配置文件的修改时，需要注意的是，使用的校验工具本身可能已经被修改过，操作系统的内核也有可能被修改了，这非常普遍。因此，建议使用一个可信任的内核启动系统，而且使用的所有分析工具都应该是干净的。

（2）检查被修改的数据

入侵者经常会修改系统中的数据，因此建议对 Web 页面文件、FTP 存档文件、用户目录下的文件以及其他的文件进行校验。

（3）检查入侵者留下的工具和数据

入侵者通常会在系统中安装一些工具，以便继续监视被入侵的系统。入侵者一般会在系统中留下如下文件：

① 网络嗅探器。

② “特洛伊木马”程序。

③ 后门。

④ 安全缺陷攻击程序：系统运行存在安全缺陷的软件是其被入侵的一个主要原因。入侵者经常会使用一些针对已知安全缺陷的攻击工具，以此获得对系统的非法访问权限。这些工具通常会留在系统中，保存在一个隐蔽的目录中。

因此，建议对系统进行彻底的搜索，找出上面列出的工具及其输出文件。

（4）审查系统日志文件

详细地审查系统日志文件，可以了解系统是如何被入侵的，入侵过程中攻击者执行了哪些操作，以及哪些远程主机访问了你的主机。通过这些信息，能够对入侵有更加清晰的认识。

（5）检查网络嗅探器

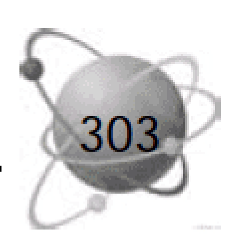
判断系统是否被安装了嗅探器，首先要看当前是否有进程使网络接口处于混杂（Promiscuous）模式下。只要任意网络接口处于混杂模式下，就表示可能系统被安装了网络嗅探器。有一些工具程序也可以帮助检测系统内的嗅探器程序。

（6）检查网络上的其他系统

除了已知被入侵的系统外，还应该对网络上所有的系统进行检查。主要检查和被入侵主机共享的网络服务（例如 NIX、NFS）或者通过一些机制（例如 hosts.equiv、rhosts 文件，或者 kerberos 服务器）和被入侵主机相互信任的系统。

（7）检查涉及到的或者受到威胁的远程站点

在审查日志文件、入侵程序的输出文件和系统被入侵以来被修改的和新建立的文件时，



要注意哪些站点可能会连接到被入侵的系统。根据经验，那些连接到被入侵主机的站点，通常也已经被入侵了。所以要尽快找出其他可能遭到入侵的系统，通知其管理人员。

4．向计算机紧急反应组 CERT 提交事件报告

中国大陆地区的网址是：http://www.cert.org.cn。填写一份事件报告表，使用电子邮件发送到 http://www.cert.org，就可以从他们那里得到一些恢复建议和更多帮助。CERT 也会根据事件报告表对攻击趋势进行分析，将分析结果总结到其安全建议和安全总结中，从而防止攻击的蔓延。

5．恢复系统

（1）安装干净的操作系统版本

如果主机被入侵，系统中的任何东西都有可能被攻击者修改，包括内核、二进制可执行文件、数据文件、正在运行的进程以及内存。此时通常需要重装操作系统，然后在重新连接到网络之前安装所有的安全补丁，只有这样才会使系统不受后门和攻击者的影响。只是找出并修补被攻击者利用的安全缺陷是不够的。

（2）取消不必要的服务

只配置系统要提供的服务，取消那些没有必要的服务。检查并确信其配置文件没有脆弱性以及该服务是否可靠。通常最保守的策略是取消所有的服务，只启动需要的服务。

（3）安装供应商提供的所有补丁

强烈建议安装所有的安全补丁，以使系统能够抵御外来攻击，不被再次侵入，这是最重要的一步。

（4）查阅 CERT 的安全建议、安全总结和供应商的安全提示。

（5）谨慎使用备份数据

从备份中恢复数据时，要确信备份主机没有被入侵。一定要记住，恢复过程可能会重新带来安全缺陷，被入侵者利用。

（6）改变密码

在弥补了安全漏洞或者解决了配置问题以后，建议改变系统中所有账户的密码，直到确信所有账户的密码都不容易被猜到。有时可能需要使用供应商提供的或者第三方的工具加强密码的安全。

6．加强系统和网络的安全

（1）根据 CERT 的 UNIX/NT 配置指南检查系统的安全性。

（2）安装安全工具。在将系统连接到网络上之前，一定要安装所有选择的安全工具。

（3）打开日志。启动日志程序，将它们设置到准确的级别。经常备份日志文件，或者将日志写到另外的机器（一个只能增加的文件系统或者一个安全的日志主机）。

（4）配置防火墙对网络进行防御。

完成以上步骤后，就可以把系统连接回 Internet 了。最后还应该升级系统的安全策略，

CERT 协调中心建议每个站点都要有自己的计算机安全策略。每个组织都有自己特殊的文化和安全需求，因此需要根据自己的情况指定安全策略。

9.5 电子邮件系统的安全

电子邮件简称 E-mail（Electronic Mail），是 Internet 上最常用的功能之一，使用户可以通过 Internet 交换邮件形式的信息文件。电子邮件不是一种“终端到终端”的服务，而是一种被称为“存储转发式”的服务。这就是说，电子邮件的发送要通过不同的路由器进行转发，直至到达电子邮件最终接收主机。因此，攻击者可以在电子邮件数据包经过路由器的时候把它们截取下来，而且发件人对邮件是否被截获也是毫不知情的。可见电子邮件系统同样面临着严峻的安全问题。

当前，电子邮件系统的发展面临着机密泄漏、信息欺骗、病毒侵扰、垃圾邮件等诸多安全问题的困扰。人们对电子邮件系统和服务的要求日渐提高，其中安全需求尤为突出。同时，国家也正在积极筹划电子签名、反垃圾邮件等电子邮件安全相关的法律、法规。

9.5.1 电子邮件的安全漏洞

使用电子邮件就像在邮局发送一封没有封口的信一样不安全。从技术上讲，没有任何方法能够阻止攻击者截取电子邮件数据包。电子邮件的收发方式一般有两种，一种是通过 Web 页方式收发邮件，即用浏览器登录到主页进行收发；另一种是使用邮件客户端，例如 Outlook 和 Foxmail 等，使用这种方法的前提是邮件服务器必须支持 POP 协议。目前，多数免费信箱都支持这两种方式，而前者则更为普遍。

下面主要就用 Web 页方式收发邮件时存在的安全漏洞作一简单介绍。

1. 缓存漏洞

对多数浏览器来说，为了提高浏览速度，系统会自动将最近浏览过的网页保存到硬盘的某个临时文件夹里，这个文件夹称为缓存。当用户打开的网页关闭时，这些文件仍然可以轻易被读取。当用户通过 Web 页面方式读信，那么这一封信实质上就是一个普通的网页，同样会被保存在缓存里。如果有人接触用户的硬盘文件，也就没有任何秘密了。

2. 历史记录漏洞

对于电子邮件系统中的每个信箱，都能将用户名和密码通过特定的算法体现在 URL 上，浏览器的历史记录里会保存这一 URL 地址。如果有些信箱没有设置超时校验，那么任何人都可以通过查看本机的历史记录而进入信箱。

3. 攻击性代码漏洞

恶意的发件人可以把一段攻击性代码包含在给用户的邮件中，当用户打开这个邮件时，

这个隐藏的程序代码便可将邮件自动转发到对邮件感兴趣的人手中。有的恶意代码可以打开无数个窗口，使系统资源耗尽而最终死机。

9.5.2　电子邮件欺骗

电子邮件欺骗行为通常是指欺骗用户进行一个毁坏性操作或暴露敏感信息。

电子邮件欺骗往往是在电子邮件中改变发送者的名字使之看起来是从某地或某人发来的，这种“欺骗”经常被诡计制造者用来防止被人们识破，还可用来实现恶作剧或恶意行为。

电子邮件欺骗会制造安全漏洞。例如，电子邮件假称来自系统管理员，要求用户将其口令改变为特定的字符串，并威胁用户如果不照此办理，将关闭用户的账户。用户就应该了解，任何系统管理人员都不会用电子邮件发出这样的要求。相反，会发出一份备忘录，或有其他的验证手段。

由于简单电子邮件传输协议 SMTP 没有验证系统，导致伪造电子邮件十分方便。如果站点允许与 SMTP 端口联系，任何人都可以与该端口联系，并以你甚至虚构的某人的名义发出电子邮件。

9.5.3　电子邮件病毒

“电子邮件病毒”其实和普通的计算机病毒一样，只不过由于它们的传播途径主要是通过电子邮件，所以才被称为“电子邮件病毒”。“电子邮件病毒”主要是为了使用户的计算机感染病毒，或者是成为黑客手中的工具。“电子邮件病毒”除了具备普通病毒可传播性、可执行性、破坏性、可触发性特征之外，还有感染速度快、扩散面广、清除困难、破坏性大、隐蔽性强等特点。

要想防范邮件病毒，必须能够准确地识别电子邮件病毒。一般情况下，可以从以下几个方面识别“电子邮件病毒”。

1. 查看附件大小

电子邮件的附件通常是“电子邮件病毒”的最佳载体，通过查看附件大小，可以识别出电子邮件是否携带病毒。例如，一般情况下，一个 Word 文档附件的大小为几十 KB 左右，如果发现电子邮件的附件是几百 KB，则该封邮件便很有可能携带了病毒。

2. 查看邮件地址

“电子邮件病毒”的传播者通常会利用一些陌生的邮件地址欺骗用户，当收到来自陌生地址的邮件时，一定要加倍小心。如果这类邮件带有附件，更要谨慎，这样的邮件有非常大的可能是病毒的携带者。对于来自陌生地址的邮件，在看了邮件地址后，再看邮件内容，如果内容是无关痛痒且与工作无关的，基本可以判断该封邮件是病毒的携带者。

3. 识别真伪退信

用户书写邮件时，如果将收件人的电子邮件地址写错了，邮件服务器会自动将该邮件退回。一些“电子邮件病毒”的传播者通常会利用伪装的退信传播病毒，因为退信中通常会有一个附件，书写着用户邮件的正文，一旦用户打开了假冒的邮件服务器系统退信，并且查看了附件，“电子邮件病毒”就会感染用户的计算机。为此，用户必须识别真伪退信。识别真伪退信的方法非常简单，看一下邮件地址即可。例如网易的退信邮件，其发件人显示为 postmaster@163.com。

4. 周密防范邮件病毒入侵

从上面的叙述可以看出，“电子邮件病毒”也是病毒的一类，但有一定的特殊性。为此，要充分利用软件的防毒功能，制定出周密的防范邮件病毒入侵的方案。例如，合理设置杀毒软件。大部分杀毒软件都能对磁盘中的文件进行实时监控，但有些杀毒软件并不具备对邮件进行实时监控的功能，为此必须为计算机安装一款对邮件实时监控能力非常强的杀毒软件。在邮件实时扫描方面，杀毒软件的邮件扫描功能启用后，收发邮件过程中就可以对邮件内容及附件进行检查，这样可以有效防止“电子邮件病毒”的入侵。

9.5.4 电子邮件加密

使用电子邮件就像在邮局发出一封没有封口的信件一样不安全。从技术上讲，没有任何方法能够阻止攻击者截获电子邮件数据包。唯一有效的办法就是让攻击者无法阅读截获的数据包，也就是对电子邮件加密。当电子邮件加密后，只要加密算法和密钥足够强大，那么即使攻击者截获了邮件数据也无法看到或修改邮件的内容。

1. 电子邮件加密方法

常用的电子邮件加密方法有以下几种：

（1）端到端的加密。就是从源设备到接收设备的完全加密。这种方法通过禁止插入点而提供最高级的安全，因为在这些插入点上纯文本数据就可以被任何人读取。加密软件必须要安装在端点上并进行维护，端点必须与客户端的电子邮件阅读软件相集成。

（2）网关到端点的加密。这是一种简化的加密，它提供了从发送方网络内的网关系统到接收端的完全加密。在这种方案中，消息以纯文本的形式从发送方的桌面发出，并在相对邻近于电子邮件服务器的网关上进行加密。这种模式取消了对任何加密软件的需要，或者取消了发送方的干预。

（3）网关到网关的加密。这种方法就像网关到端点的加密，不过它在接收方一端增加了一个加密网关，从而也就无须桌面软件和管理成本。但这种加密成本极高，且收发双方必须在同一加密网关内。

（4）网关到 Web 的加密。可以通过一个 Web 服务器提供对敏感数据的访问。数据通常是通过传输层加密来加以保护的，例如使用加密套接字协议层 SSL。这就保证了与任何

接收方的通信安全，而不管其架构或复杂水平。在这种方案中，一个标准的消息被发往接收端，并通知它有一个安全消息正在网关处等待。接收方通过一个安全连接找到这个消息，这需要通过由不同频道信号传输（Out-Of-Band）机制提供的机密信息进行身份验证。

2．实现加密的原理

（1）实现加密的原理

电子签名技术采用多种加密方法，在此通过易于理解的 RSA 公钥体系为例简述其原理。RSA 加密基于一个对大数进行分解质因子非常困难的数学假设，使用 2 个大素数的函数，一个作为公钥，另一个作为私钥。由于这 2 个密钥是互补的，公钥加密的密文可以用私钥解密，反之亦然。因而邮件发送者只需要使用收件人的公钥加密邮件，加密后的邮件只有拥有私钥的收件人才可能有办法解密阅读，也就实现了邮件的加密，从而保证了邮件不会被任何第三者所阅读，即使在传输的过程中被第三者截取仍然不至于泄密。

（2）电子邮件加密的原理

当用户使用自己的电子证书在发出的邮件上签名时，邮件将被按照邮件的内容通过摘要函数运算取得一个可以用以检验邮件完整性的值，并将该值使用电子证书中的私钥加密，然后与公钥和邮件内容一起发送出去。由于私钥加密的内容只有对应的公钥可以解密，并且摘要函数可以在任意大小的数据中采集一个固定长度的摘要，供采集的数据源即使有一位数据改变取得的结果也不同，邮件的内容有任何改变都无法与原来检验邮件完整性的值相匹配，当收件人收到邮件时就可知道邮件的内容是否被篡改，同时也知道该邮件发送者使用的是哪一个电子证书。而由于第三方的权威证书发行机构在发出电子证书时，将验证申请者是否拥有所申请电子邮箱的使用权，收件人也就能够通过证书发行机构验证发件人所使用的电子证书，确认所收到的邮件的确来自拥有这个邮箱地址的用户，从而实现对发件人的真实性与邮件内容是否完整的鉴别。

电子签名技术非常复杂，但使用起来非常方便，不论是签名还是加密、解密，具体的步骤都将由电子邮件客户端软件实施。目前 FoxMail、Outlook Express 与 Outlook 等主流的电子邮件客户端软件都能够支持。用户需要做的只是申请电子证书，并在电子邮件客户端软件上指定每个电子邮件地址将使用哪种电子证书。在需要为发送的电子邮件签名或加密时，单击相应的按钮即可完成。而当收到使用电子签名的邮件时，验证邮件是否完整和解密的工作也将由电子邮件客户端软件自动完成。

9.5.5　电子邮件加密软件 PGP 的应用举例

PGP 的全称是 Pretty Good Privacy，是 Internet 上一个著名的共享加密软件。PGP 与具体的应用无关，可独立提供数据加密、数字签名、密钥管理等功能，适用于电子邮件内容的加密和文件内容的加密；也可作为安全工具嵌入到应用系统之中。目前，PGP 已经是事实上进行电子信息加密的应用标准，IETF 在安全领域有一个专门的工作组负责进行 PGP 的标准化工作，许多大的公司、机构，包括很多安全部门在内，都拥有自己的 PGP 密码。

PGP 的传播和使用处于一种无政府状态，完全由使用者自行控制掌握，通过数字签名

所形成的信任链将彼此信任的用户关联起来。也就是说，PGP 没有外部约束，每个人自行决定信任谁。如果用户比较小心谨慎，而且使用对象限制在一定范围，则 PGP 安全就可以得到保证，因为信任链是由用户自己维护控制的，不必依赖于一个自己无法控制的外部系统。当然，也正因为密钥管理系统的这种自维护性，PGP 的密钥管理存在缺乏规范标准、缺乏权威和缺乏仲裁等问题。

1. PGP 的工作方式

PGP 使用了以下一些算法：RSA、AES、CAST、IDEA、TripleDES、Twofish、MD5．ZIP、PEM 等。PGP 使用 RSA 算法对 IDEA 密钥进行加密，然后使用 IDEA 算法对信息本身进行加密。在 PGP 中使用的信息摘要算法是 MD5。

由于 PGP 也为电子邮件提供数据安全服务，为了克服一些 SMTP 只支持 7bit 传输的问题，PGP 对传输的信息提供了编码功能（定义在 RFC 1113 中）。为了减少由于编码所造成的传输内容长度增加，PGP 在传输数据之前，先使用 ZIP 技术对数据进行压缩，通常可减少近 50%的长度。由于加密本身会使文件的相关性降低，影响压缩的效率，因此 PGP 是在加密前对信息进行压缩，这样还可以减少加密的信息长度。

PGP 至少为每个用户定义两个密钥文件，称为 Keyring，分别存放自己的私钥（可以不止一个）和自己及其他用户的公钥。

2. PGP 应用举例

以 PGP 8.1 版为例，下载安装文件后执行安装，然后重启计算机 PGP 将以向导的方式指引用户一步步产生自己的公钥/私钥对（若已有，则也可直接指定公钥/私钥文件所在的文件夹导入使用），生成时要求用户输入通行码（Passphrase），如图 9-8 所示。

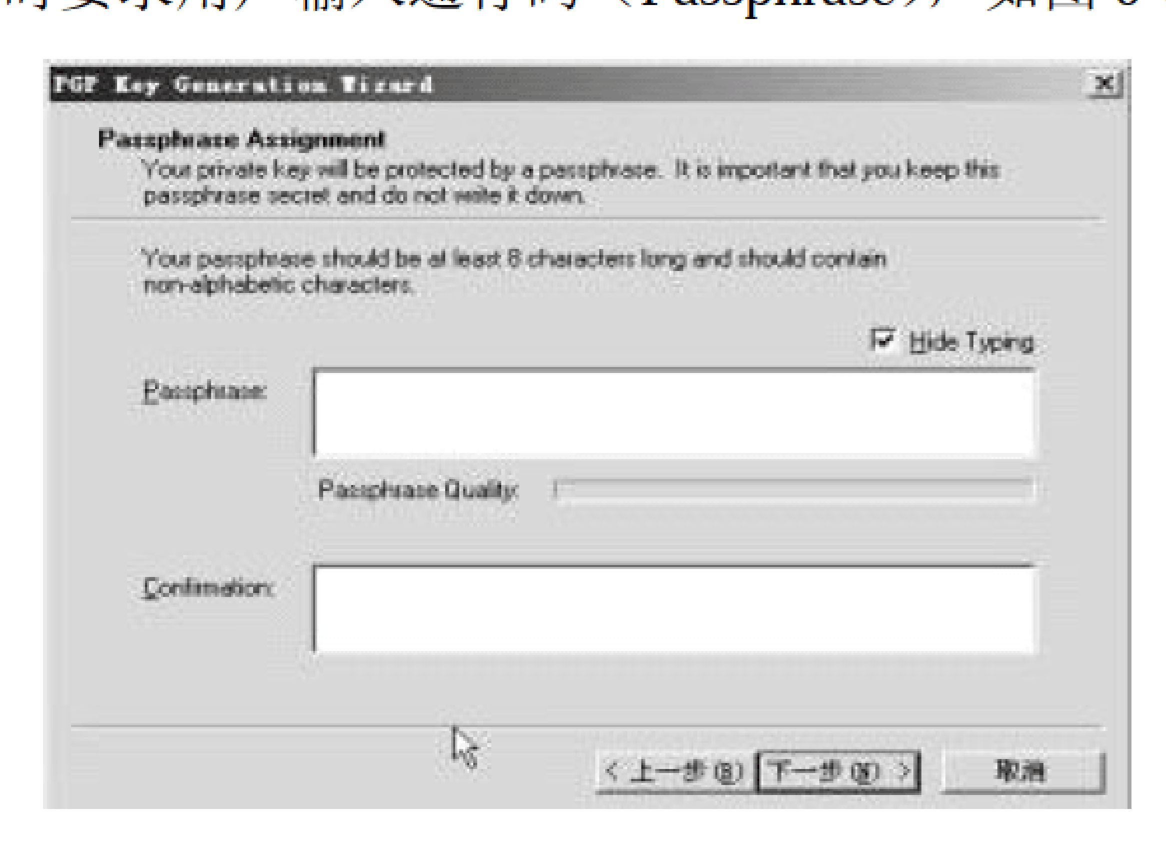


图 9-8　PFP 用户输入通行码窗口

PGP 运行后，在系统提示区的图标为 。PGP 的主要功能如图 9-9 所示。

（1）PGP 的主要功能

① 密钥管理（PGPkeys）

管理界面如图 9-10 所示。可新建、导入、导出密钥，建立相互间信任链。

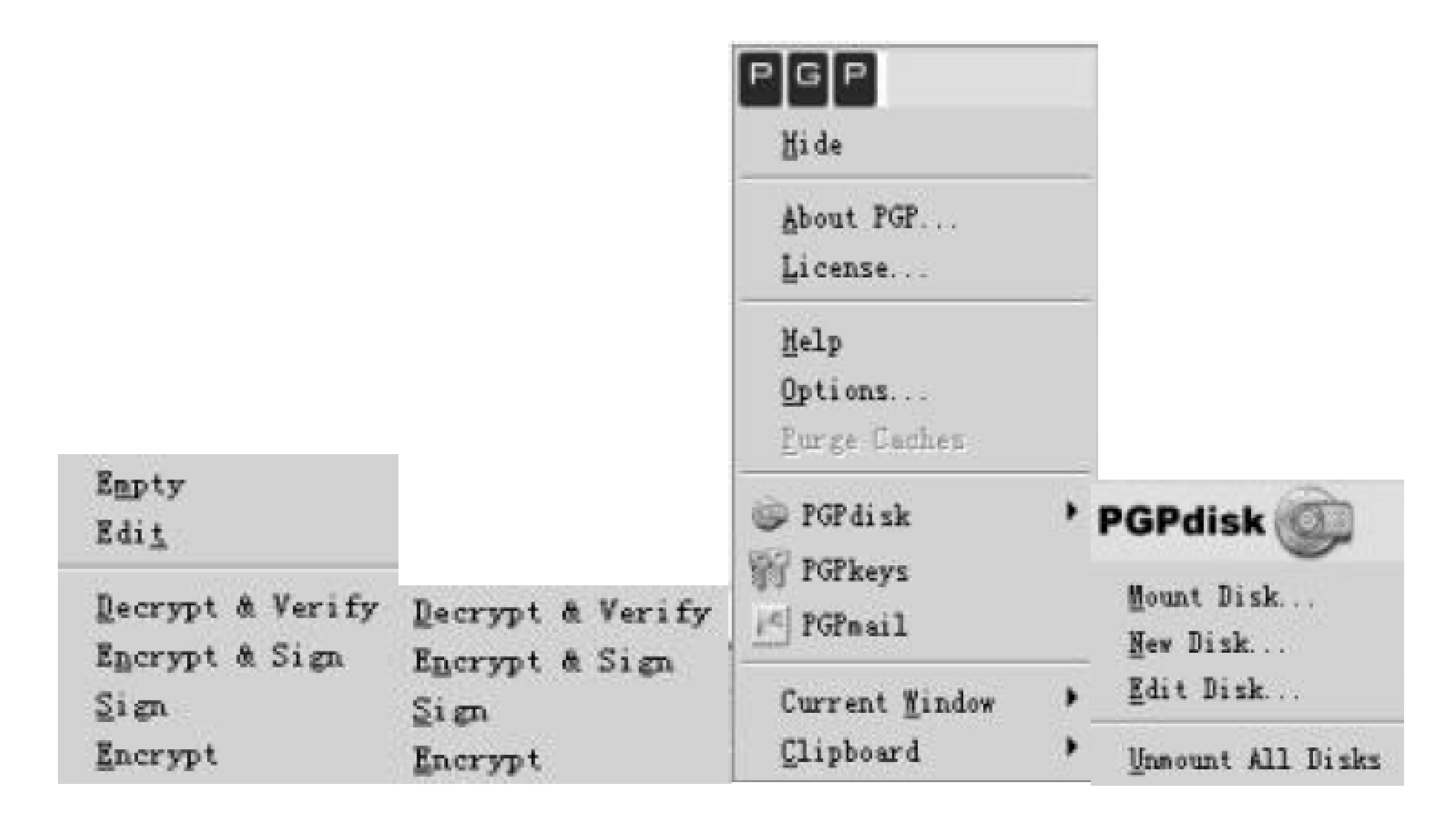


图 9-9　PGP 主要功能

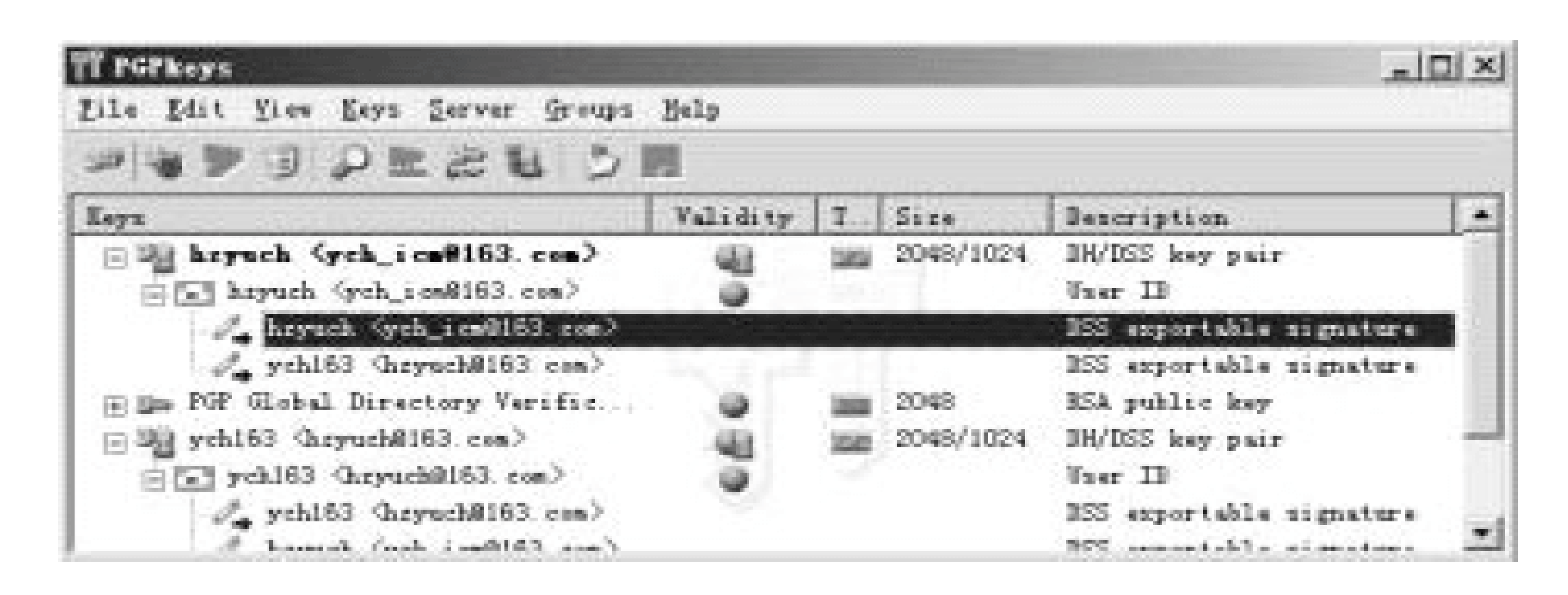


图 9-10　密钥管理

② 剪切板信息加/解密

可实现剪切板信息的加密、认证、加密并认证、解密等操作。

③ 当前窗口信息加/解密

可实现当前窗口信息的加密、认证、加密并认证、解密等操作。

④ 文件的加/解密与安全删除（PGPmail）

可对文件独立进行加/解密。PGPmail 工具栏如图 9-11 所示。

⑤ PGP 加密磁盘（PGPdisk）

可在物理硬盘中划出一块区域，由 PGP 作为一个虚拟磁盘进行管理。使用时打开，使用完毕加密关闭。

（2）在 Outlook 用 PGP 发送加密文件

若要发送加密的电子邮件，在写邮件时必须单击 Encrypt Message（PGP）按钮使其处于按下状态，如图 9-12 所示。

单击“发送”按钮后，将提示选择加密用的公钥。若本地无指定公钥，则将自动搜索 PGP 的公钥发布中心。用户接收到加密的电子邮件后，可在 Outlook 工具栏中单击 Decrypt Message（PGP）按钮进行解密，解密时要求提供通行码。也可以通过附件发送加密后的文件，文件一般用 PGPmail 实现加/解密。



图 9-11 PGPmail 工具栏



图 9-12 用 Outlook 发送加密邮件

9.6 虚拟专用网

虚拟专用网（Virtual Private Network，VPN）是指将物理上分布在不同地点的网络通过公用网络连接而成逻辑上的虚拟子网，并采用认证、访问控制、机密性、数据完整性等在公众网络上构建专用网络的技术，使得数据通过安全的“加密隧道”在公用网络中传播。也就是利用公用网络（通常是因特网）建立一个临时的、安全的连接，形成一条穿过混乱的公用网络的安全、稳定的隧道，是对企业内部网的扩展。在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公用网的资源动态组成的。虚拟专用网不是真的专用网络，但却能实现专用网络的功能。

9.6.1 VPN 的基本原理

VPN 是在公用网中形成的企业专用链路。为了形成这样的链路，采用了所谓的“隧道”技术，如图 9-13 所示。可以模仿点对点连接技术，依靠 Internet 服务提供商 ISP 和其他的网络服务提供商 NSP 在公用网中建立自己专用的“隧道”，让数据包通过这条隧道传输。对于不同的信息来源，可分别给它们开出不同的隧道。

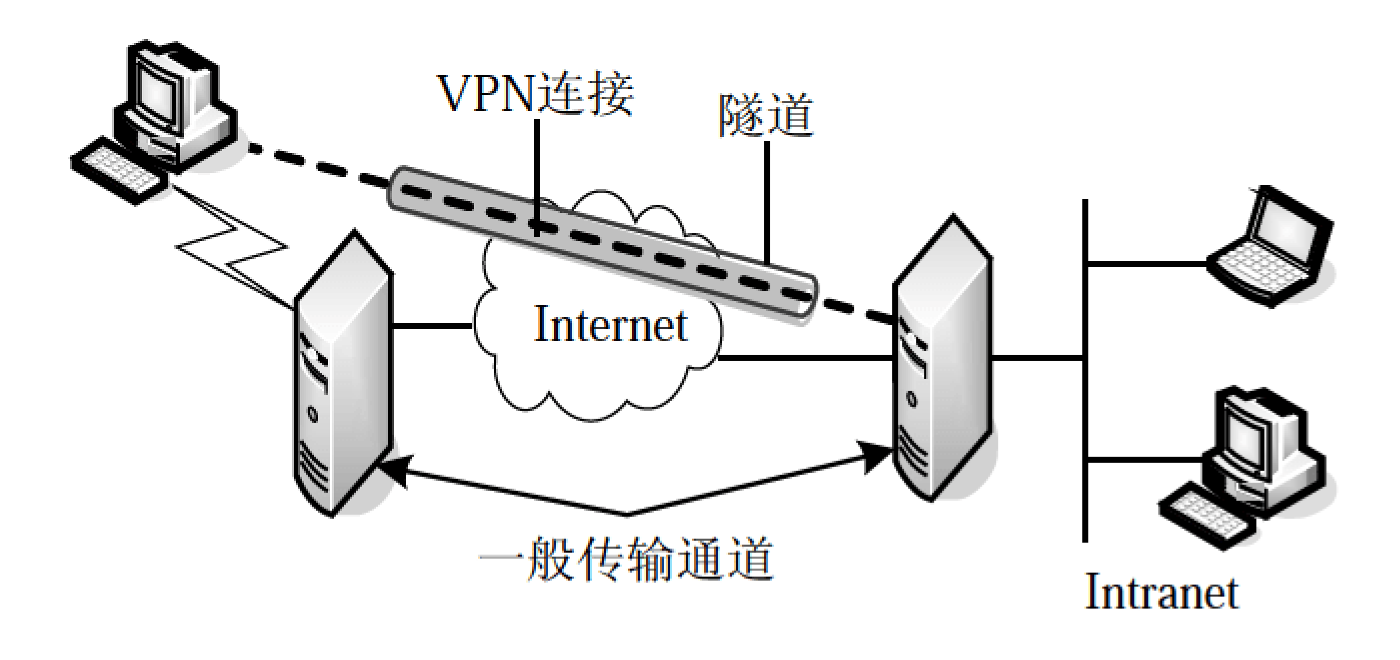
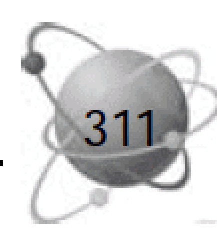


图 9-13 VPN 的隧道技术

这里的“隧道”是指一种利用公用网设施，在一个网络之中的“网络”上传输数据的方法，被传输的数据可以是另一种协议的数据帧。隧道协议利用附加的报头封装帧，附加



的报头提供了路由信息，因此封装后的包能够通过中间的公用网。封装后的数据包所途经的公用网的逻辑路径称为隧道。一旦封装的帧到达了公用网上的目的地，帧就会被解除封装并被继续送到最终目的地。具体过程如图 9-14 所示。

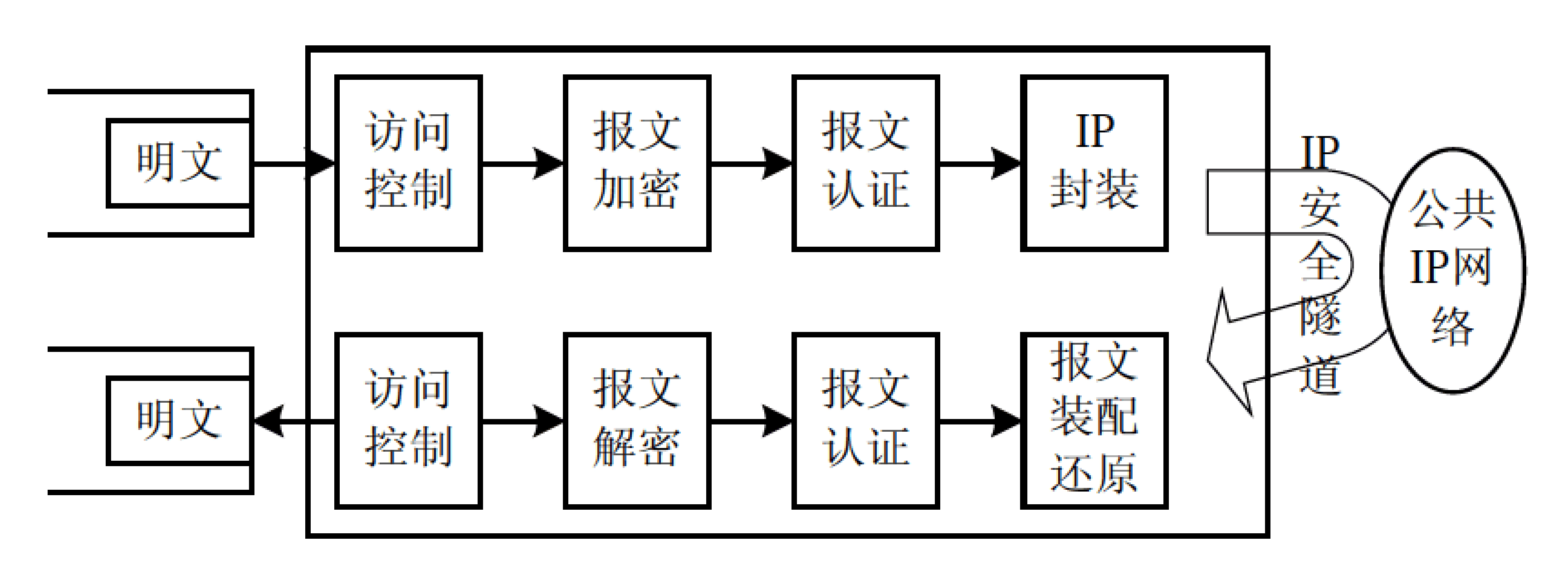


图 9-14　IP-VPN 工作原理

VPN 网络中通常还有一个或多个安全服务器。安全服务器除提供防火墙和地址转换功能之外，还通过与隧道设备的通信来提供加密、身份验证和授权功能。它们通常也提供各种信息，例如带宽、隧道端点、网络策略和服务等。

虚拟专用网一般应提供如下安全功能：

（1）加密数据，以保证通过公用网传输的信息即使被他人截获也不会泄露。

（2）信息认证和身份认证，保证信息的完整性、合法性，并能鉴别用户的身份。

（3）提供访问控制，不同的用户有不同的访问权限。

（4）地址管理。VPN 方案必须能够为用户分配专用网络上的地址，并确保地址的安全性。

（5）密钥管理。VPN 方案必须能够生成并更新客户端和服务器的加密密钥。

（6）多协议支持。VPN 方案必须支持因特网上普遍使用的基本协议，包括 IP、IPX 等。

9.6.2　VPN 的应用环境

根据服务类型，VPN 业务大致可分为 3 类。此处引用 Cisco 的定义方式，将 3 种用户需求定义为 Intranet VPN、Access VPN 与 Extranet VPN，分别应用在不同的网络服务环境中。

1．内部网 VPN（Intranet VPN）

内部网即企业的总部与分支机构间通过公用网构筑的虚拟网。这种类型的连接带来的风险最小，因为公司通常认为其分支机构是可信的，并将它作为公司网络的扩展。内部网 VPN 的安全性取决于两个 VPN 服务器之间的加密和验证手段。如图 9-15 所示为一典型的内部网 VPN。

2．远程访问 VPN（Access VPN）

远程访问又称为拨号 VPN（即 VPDN），是指企业员工或企业的小分支机构通过公用网以远程拨号的方式构筑的虚拟网。如图 9-16 所示，典型的远程访问 VPN 是用户通过本

地的信息服务供应商 ISP 登录到因特网上，并在所在的办公室和公司内部网之间建立一条加密信道。

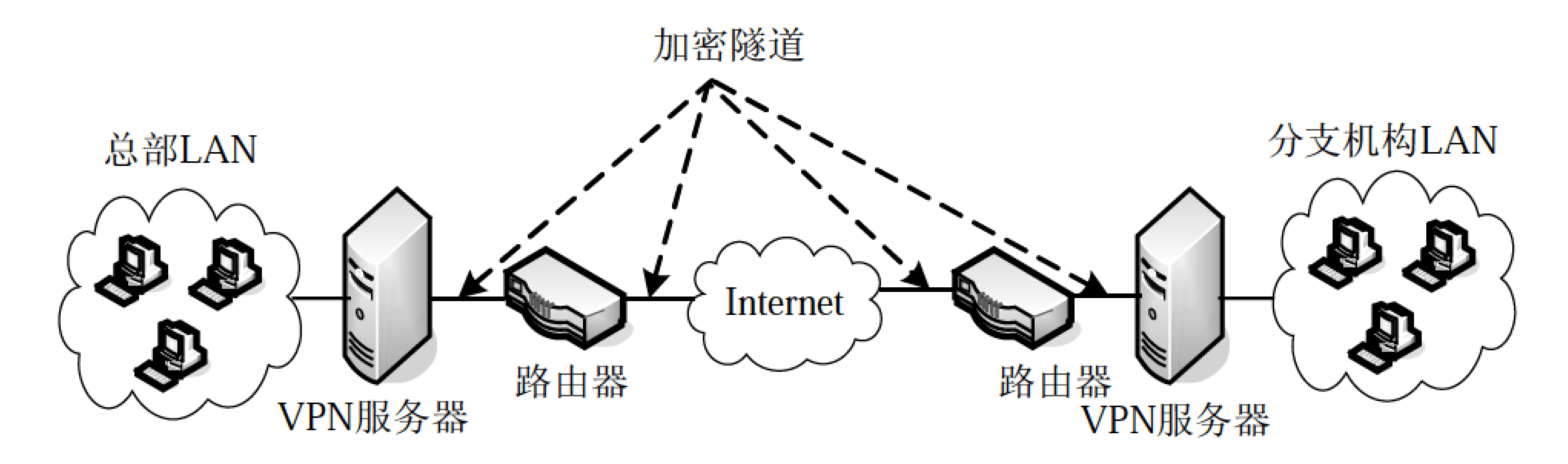


图 9-15 内部网 VPN

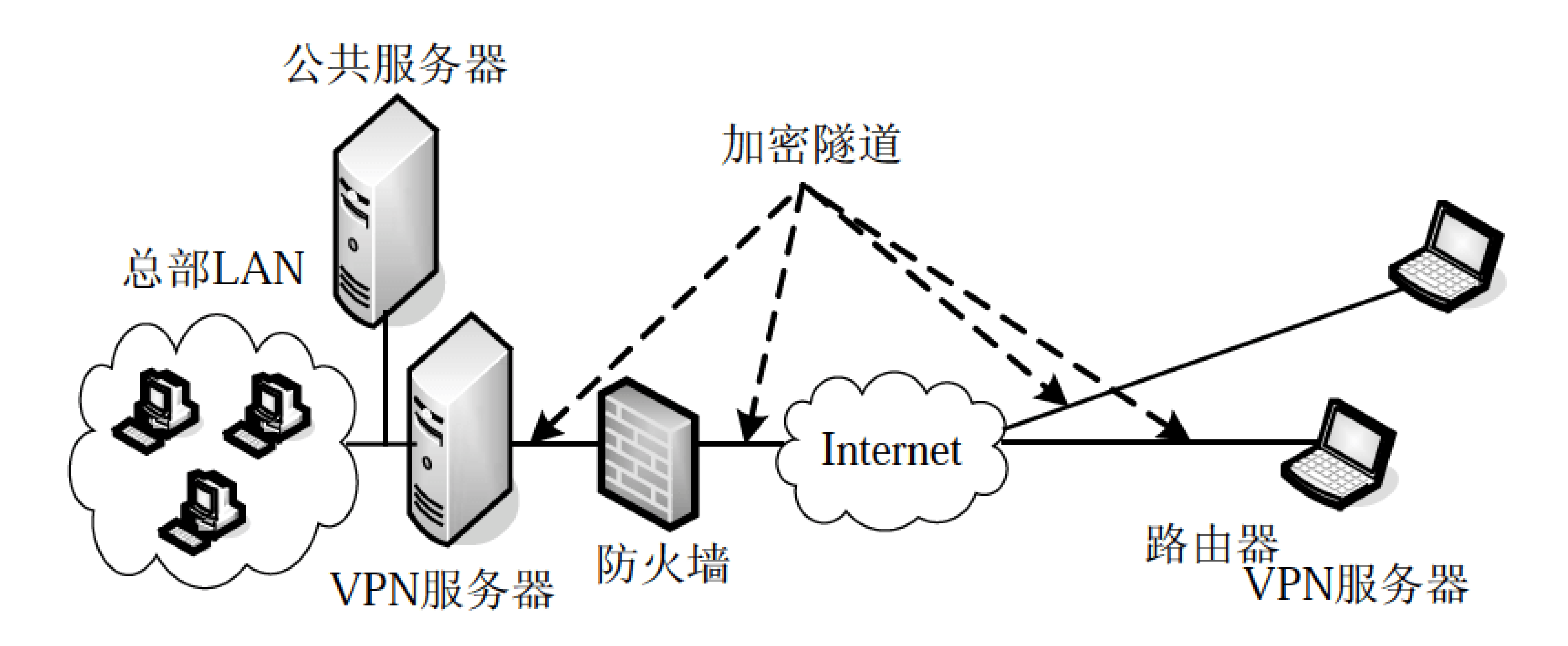


图 9-16 远程访问 VPN

公司往往制定一种“透明的访问策略”，雇员即使身处远方也能像他们坐在公司总部的办公室里一样自由地访问公司的资源；为方便雇员的使用，远程访问 VPN 的客户端应尽量简单，同时考虑加密、身份验证过滤等方法的使用。

3. 外联网 VPN（Extranet VPN）

外联网即企业间发生收购、兼并或企业间建立战略联盟后，不同企业网通过公用网来构筑的虚拟网，如图 9-17 所示。它能保证包括 TCP 和 UDP 服务在内的各种应用服务的安全，例如 E-mail、HTTP、FTP、RealAudio、数据库的安全以及一些应用程序（例如 Java、ActiveX）的安全。

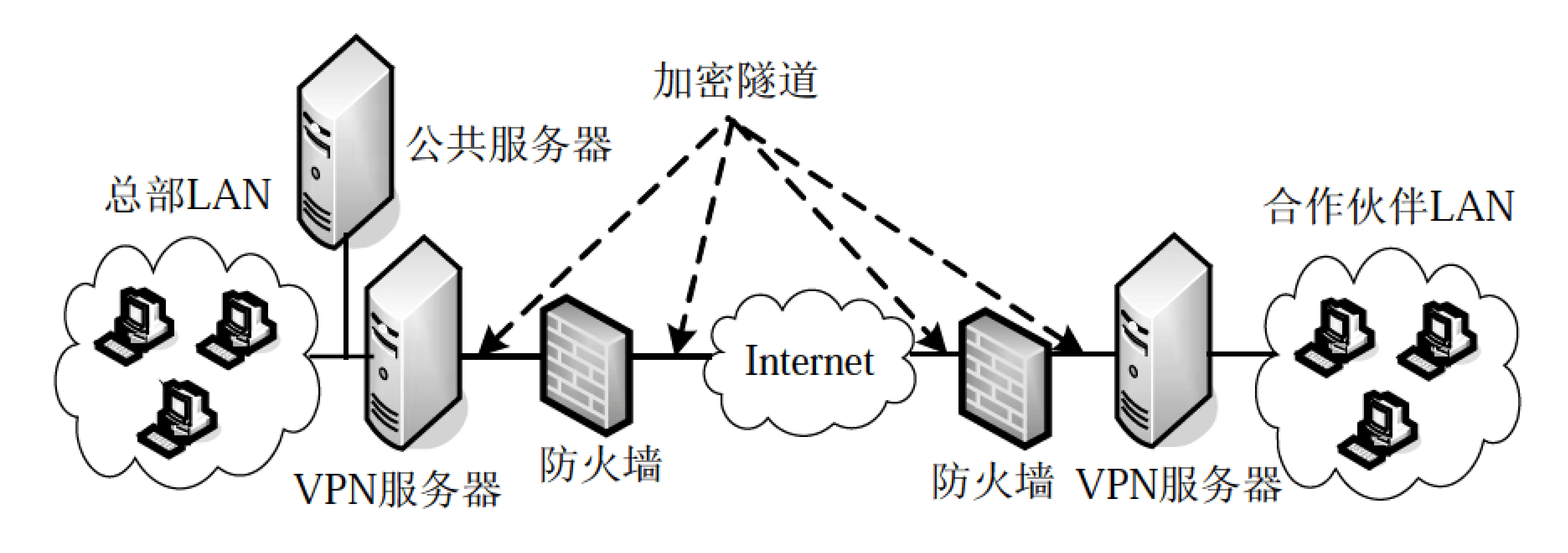


图 9-17 外联网 VPN

通常把 Intranet VPN 和 Extranet VPN 统称为专线 VPN。

9.6.3　VPN 协议

VPN 区别于一般网络互联的关键在于“隧道”的建立，数据包经过加密后，按隧道协议进行封装、传送以保证其安全性。VPN 中的隧道是由隧道协议形成的，那么 VPN 中的关键就是隧道协议。VPN 使用的隧道协议主要有 3 种：点到点隧道协议 PPTP、第二层隧道协议 L2TP 以及 IPSec。PPTP 协议允许对 IP、IPX 或 NetBEUI 数据流进行加密，然后封装在 IP 包头中通过企业 IP 网络或因特网发送。L2TP 协议允许对 IP、IPX 或 NetBEUI 数据流进行加密，然后通过支持点对点数据报传递的任意网络发送，例如 IP、X.25、帧中继或 ATM。IPSec 隧道模式允许对 IP 负载数据进行加密，然后封装在 IP 包头中通过企业 IP 网络或公共 IP 因特网发送。本节只对 PPTP 协议和 L2TP 协议作一简单介绍，关于 IPSec 可参阅 9.7 节。

1. 点到点隧道协议 PPTP

PPP 协议主要是设计用来通过拨号或专线方式建立点对点连接发送数据，因此适合用于远程访问虚拟专用网。1996 年，Microsoft 和 Ascend 等在 PPP 协议的基础上开发了 PPTP（Point-to-Point Tunneling Protocol），将它集成在 Windows NT Server 4.0 中，Windows NT Workstation 和 Windows 9.x 也提供了相应的客户端软件。PPTP 支持多种网络协议，可把 IP、IPX、AppleTalk 或 NetBEUI 的数据包封装在 PPP 包中，再将整个报文封装在 PPTP 隧道协议包中，最后再嵌入 IP 报文、帧中继或 ATM 中进行传输。PPTP 提供流量控制，减少拥塞的可能性，尽量避免由包丢弃而引发包重传的数量。PPTP 的加密方法采用 Microsoft 点对点加密 MPPE（Microsoft Point-to-Point Encryption）算法，可以选用较弱的 40 位密钥或强度较大的 128 位密钥。

2. 第二层隧道协议 L2TP

1996 年，Cisco 提出 L2F（Layer 2 Forwarding）隧道协议。它也支持多协议，但其主要用于 Cisco 的路由器和拨号访问服务器。1997 年底，Micorosoft 和 Cisco 公司把 PPTP 协议和 L2F 协议的优点结合在一起，形成了 L2TP（Layer 2 Tunneling Protocol）协议。

L2TP 协议综合了 PPTP 协议和 L2F 协议的优点，并且支持多路隧道，这样可以使用户同时访问 Internet 和企业网。

PPTP 是一个数据链路层的协议，而 L2TP 是一种网络层协议，支持封装的 PPP 帧在 IP、X.25、帧中继或 ATM 等网络上进行传送。当使用 IP 作为 L2TP 的数据报传输协议时，可以使用 L2TP 作为 Internet 网络上的隧道协议。

3. PPTP 与 L2TP 的区别

PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加附加包头用于数据在因特网上的传输。两个协议功能相似，但有以下几个方面的不同。

（1）PPTP 要求因特网为 IP 网络，L2TP 只要求隧道媒介提供面向数据包的点对点的

连接。L2TP 可以在 IP（使用 UDP）、帧中继永久虚拟电路（PVCs）、X.25 虚拟电路（VCs）或 ATM VCs 网络上使用。

（2）PPTP 只能在两端点间建立单一隧道，而 L2TP 支持在两端点间使用多隧道。使用 L2TP 时，用户可以针对不同的服务质量创建不同的隧道。

（3）L2TP 可以提供包头压缩。当压缩包头时，系统开销占用 4 个字节，而 PPTP 协议要占用 6 个字节。

（4）L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，不需要在第二层协议上验证隧道。

9.7 IPSec

IPSec 在 IP 层提供安全服务，使得系统能够按需选择安全协议，决定服务所使用的算法及放置需求服务所需密钥到相应位置，通常用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。IPSec 可提供的安全服务集包括访问控制、无连接的完整性、数据源认证、拒绝重发包（部分序列完整性形式）、保密性和有限传输流保密性。

IPSec 可在以下 3 个不同的安全领域使用：虚拟专用网络 VPN、应用级安全以及路由安全。目前，IPSec 主要用于 VPN。在应用级安全或路由安全中使用时，IPSec 还不是一个完全的解决方案，必须与其他安全措施配合才能更具效率，从而妨碍了它在这些领域的部署。

图 9-18 说明了 IPSec 的一个典型应用场景。一个组织的多个 LAN 不在同一地点，每个 LAN 内部的通信不需要特殊的保护，而 LAN 同不可信网络间的通信可用防火墙进行保护。我们生活在一个分布式的和移动着的世界，要在不同地点通过 Internet 访问这些 LAN 提供的服务，访问的安全性就要由 IPSec 来保证。图中工作站、服务器及路由器或防火墙等网络设备中运行了 IPSec 协议。工作站为访问 LAN，先同网络设备之间建立 IPSec 隧道，保护后续的所有会话。隧道建立后，工作站可与安全网关后的设备进行多次会话。穿过 Internet 的 IP 包受 IPSec 保护，而传递过程与普通 IP 包一样。

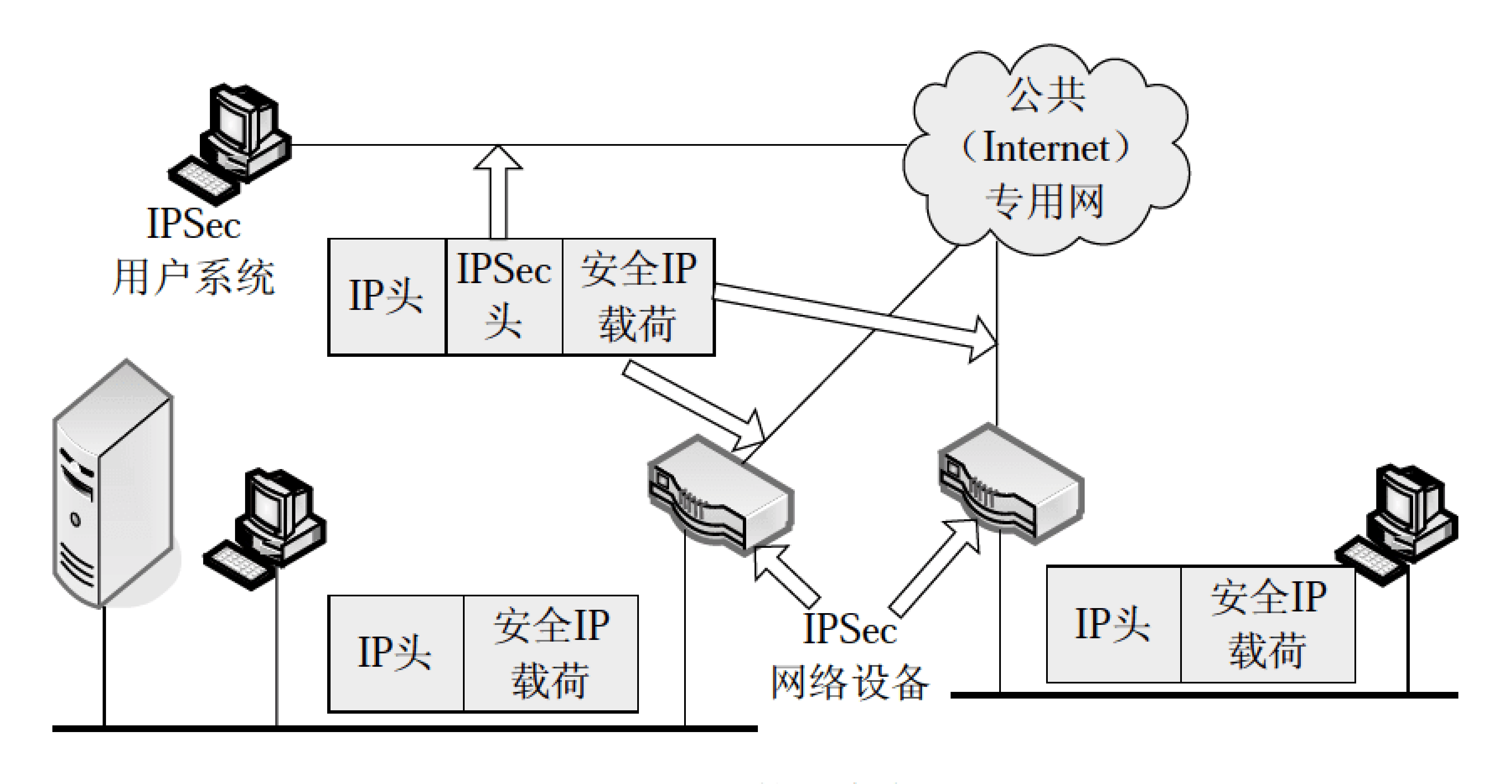


图 9-18　IPSec 的一个应用场景

9.7.1　IP 安全性分析

TCP/IP 协议簇提供了一个开放式协议平台，正将越来越多的部门和人员用网络连接起来，网络正在快速地改变着我们工作和生活的方式，但是安全性的缺乏减慢了联网的发展速度。目前网络面临的各种威胁包括保密数据的泄露、完整性的破坏、身份伪装和拒绝服务等。而目前占统治地位的 TCP/IP 协议是 IPv4，它在设计之初并没有考虑安全性，只是为数据通信而设计。而在 TCP/IP 协议的体系结构中，除了数据链路层外，TCP/IP 所有协议的数据都是以 IP 数据报的形式传输的，IP 数据报本身不具备任何安全特性，从而导致在网络上传输的数据很容易受到各种各样的攻击。因此，对通信双方不能保证收到的 IP 数据报的真实性成为 IPv4 最大的安全缺陷。

为实现 IP 网络上的安全，从 1995 年开始，IETF 建立了一个 Internet 安全协议工作组负责 IP 安全协议和密钥管理机制的制定。经过几年的努力，该工作组提出一系列的协议，构成一个安全体系，总称为 IP Security Protocol，简称为 IPSec。IPSec 是 IPv6 的一个组成部分，也是 IPv4 的一个可选扩展协议。IPSec 弥补了 IPv4 在协议设计时缺乏安全性考虑的不足。

IPSec 定义了一种标准的、健壮的以及包容广泛的机制，可用它为 IP 及其上层协议提供安全保证。IPSec 的目标是为 IPv4 和 IPv6 提供具有较强的互操作能力、高质量和基于密码的安全功能，在 IP 层实现多种安全服务，包括访问控制、数据完整性、数据源验证、抗重播、机密性等。IPSec 通过支持一系列加密算法，例如 DES、三重 DES、IDEA、AES 等，确保通信双方的机密性。

可以把 IPSec 想象成是位于 TCP/IP 协议栈的下层协议。该层由每台机器上的安全策略和发送、接收方协商的安全关联（Security Association，SA）进行控制。安全策略由一套过滤机制和关联的安全行为组成。如果一个数据包的 IP 地址、协议、端口号满足一个过滤机制，那么这个数据包将要遵守关联的安全行为。

IPSec 结合密码保护服务、安全协议组和动态密钥管理来实现上述两个目标，不仅能为企业局域网与拨号用户、域、网站、远程站点以及 Extranet 之间的通信提供强有力且灵活的保护，而且还能用来筛选特定数据流。IPSec 基于一种端对端的安全模式，这种模式有一个基本前提假设，就是假定数据通信的传输媒介是不安全的，因此通信数据必须经过加密，而掌握加/解密方法的只有数据流的发送端和接收端，两者各自负责相应的数据加/解密处理，而网络中其他只负责转发数据的路由器或主机无须支持 IPSec。

IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构。IPSec 主要包括两个安全协议——AH（Authentication Header）和 ESP（Encapsulating Security Payload）及密钥管理协议（Internet Key Exchange，IKE）。AH 提供无连接的完整性、数据发起验证和重放保护；ESP 还可另外提供加密；密钥管理协议 IKE 提供安全可靠的算法和密钥协商。这些机制均独立于算法，这种模块化的设计允许只改变不同的算法而不影响实现的其他部分。协议的应用与具体加密算法的使用取决于用户和应用程序的安全

性要求。

IPSec 的安全特性主要有：

（1）不可否认性。不可否认性可以证实消息发送方是唯一可能的发送者，发送者不能否认发送过消息。不可否认性是采用公钥技术的一个特征，当使用公钥技术时，发送方用私钥产生一个数字签名随消息一起发送，接收方用发送者的公钥来验证数字签名。由于在理论上只有发送者才唯一拥有私钥，也只有发送者才可能产生该数字签名，所以只要数字签名通过验证，发送者就不能否认曾发送过该消息。但不可否认性不是基于认证的共享密钥技术的特征，因为在基于认证的共享密钥技术中，发送方和接收方掌握相同的密钥。

（2）反重播性。反重播确保每个 IP 包的唯一性，保证信息万一被截取复制后，不能再被重新利用、重新传输回目的地址。该特性可以防止攻击者截取破译信息后，再用相同的信息包冒取非法访问权（即使这种冒取行为发生在数月之后）。

（3）数据完整性。防止传输过程中数据被篡改，确保发出数据和接收数据的一致性。IPSec 利用 Hash 函数为每个数据包产生一个加密校验和，接收方在打开包前先计算校验和，若包遭篡改导致校验和不相符，数据包即被丢弃。

（4）数据可靠性。在传输前，对数据进行加密，可以保证在传输过程中，即使数据包遭截取，信息也无法被读取。该特性在 IPSec 中为可选项，与 IPSec 策略的具体设置相关。

（5）认证。数据源发送信任状，由接收方验证信任状的合法性，只有通过认证的系统才可以建立通信连接。

9.7.2 安全关联

1. 什么是安全关联

安全关联 SA 是终结点为建立安全会话而协商的身份验证与加密方法的集合，是两个应用 IPSec 实体（主机、路由器）间的一个单向逻辑连接，用来决定保护什么、如何保护以及谁来保护通信数据。它规定了用来保护数据包安全的 IPSec 协议、转换方式、密钥以及密钥的有效存在时间等。SA 连接是单向的，要么对数据包进行“进入”保护，要么进行“外出”保护。SA 用一个三元组（安全参数索引 SPI、IP 目的地址、安全协议）唯一标识。

（1）安全参数索引（Security Parameters Index，SPI）：分配给 SA 的一个位串，只在本地有效。SPI 在 AH 和 ESP 报头中出现，使得接收系统选择 SA 并在其下处理一个收到的报文。

（2）IP 目的地址：这是 SA 的目标终点地址，也可能是最终用户系统或网络系统，例如防火墙或路由器。

（3）安全协议标识符（Security Protocol Identifier，SPI）：表明关联是 AH 或 ESP 安全关联。

因此，在任何 IP 包中，SA 都是通过 IPv4 或 IPv6 报头中的目标地址和封装扩展报头（AH 或 ESP）中的 SPI 唯一标识的。

2. SA 的作用

SA 提供的安全服务取决于所选的安全协议（AH 或 ESP）、SA 模式、SA 作用的两端点和安全协议所要求的服务。

例如，AH 为 IP 数据报提供数据源验证和无连接完整性；此外，AH 还提供了抗重播服务。接收端是否需要这一服务，可自行决定。AH 不对数据包进行加密，ESP 则可提供加密和验证以及抗重播服务。ESP 验证的数据不包括外部 IP 头，加密和验证服务至少选择其中之一。

ESP 为 SA 的加密服务提供了有限业务流机密性：隧道模式隐藏了数据包的源地址和最终目的地址；ESP 数据包填充后，隐藏了数据包的真实大小，进而隐藏了其通信特征。移动用户的 IP 地址是动态分配的，通过与公司的作为网关使用的防火墙间建立隧道模式 ESP SA，也可实现业务流的机密性。

3. SA 的管理

SA 管理的两大任务就是创建和删除。SA 的管理既可手工进行，也可通过 IKE 来完成。

手工方式下，安全参数由管理员按安全策略手工指定、手工维护。但是，手工维护容易出错，而且手工建立的 SA 没有生存周期限制，一旦建立了，就不会过期，除非手工删除。

SA 的自动建立和动态维护是通过 IKE 进行的。如果安全策略要求建立安全、保密的连接，但却不存在相应的 SA，IPSec 的内核则启动或触发 IKE 协商。

9.7.3 IPSec 模式

IPSec 有两种模式——传输模式和隧道模式。传输模式只对 IP 分组应用 IPSec 协议，对 IP 报头不进行任何修改，只能应用于主机对主机的 IPSec 虚拟专用网 VPN 中。隧道模式中，IPSec 将原有的 IP 分组封装成带有新的 IP 报头的 IPSec 分组，这样原有的 IP 分组就被有效地隐藏起来了。该模式主要应用于主机到网关的远程接入的情况。

1. 传输模式

传输模式主要用于主机或充当主机的设备之间的端对端连接。在传输模式中，AH 和 ESP 保护的是传输头。在这种模式中，AH 和 ESP 会拦截从传输层到网络层的数据包，并根据具体的配置提供安全保护。只有在要求端到端的安全保障时，才能使用 IPSec 的传输模式。

从图 9-19 可以看出传输模式是如何影响 AH IPSec 连接的：第 3 层以及第 4 层协议头被分开，在它们之间添加了 AH；认证可以保护原始 IP 协议头中除了可变字段以外的其他部分。

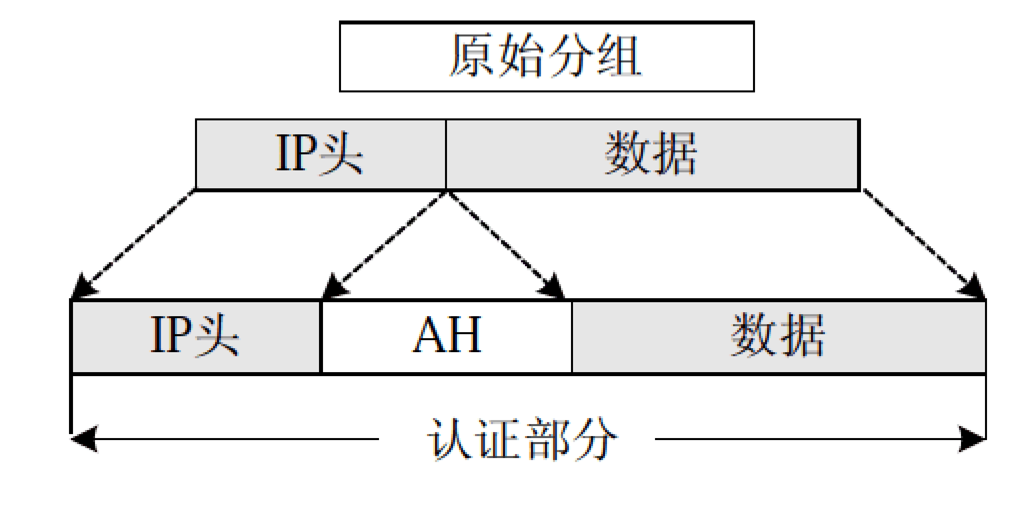


图 9-19 AH 传输模式

图 9-20 给出了 ESP 传输模式。同样，IP 协议头被调整到数据报左边，并插入 ESP 协议头。

ESP 协议尾以及完整性检查值（Integrity Check Value，ICV）附加在数据报末端。如果需要加密（在 AH 中无效），仅对原始数据和新的 ESP 协议尾进行加密。认证从 ESP 协议头一直延伸到 ESP 协议尾。

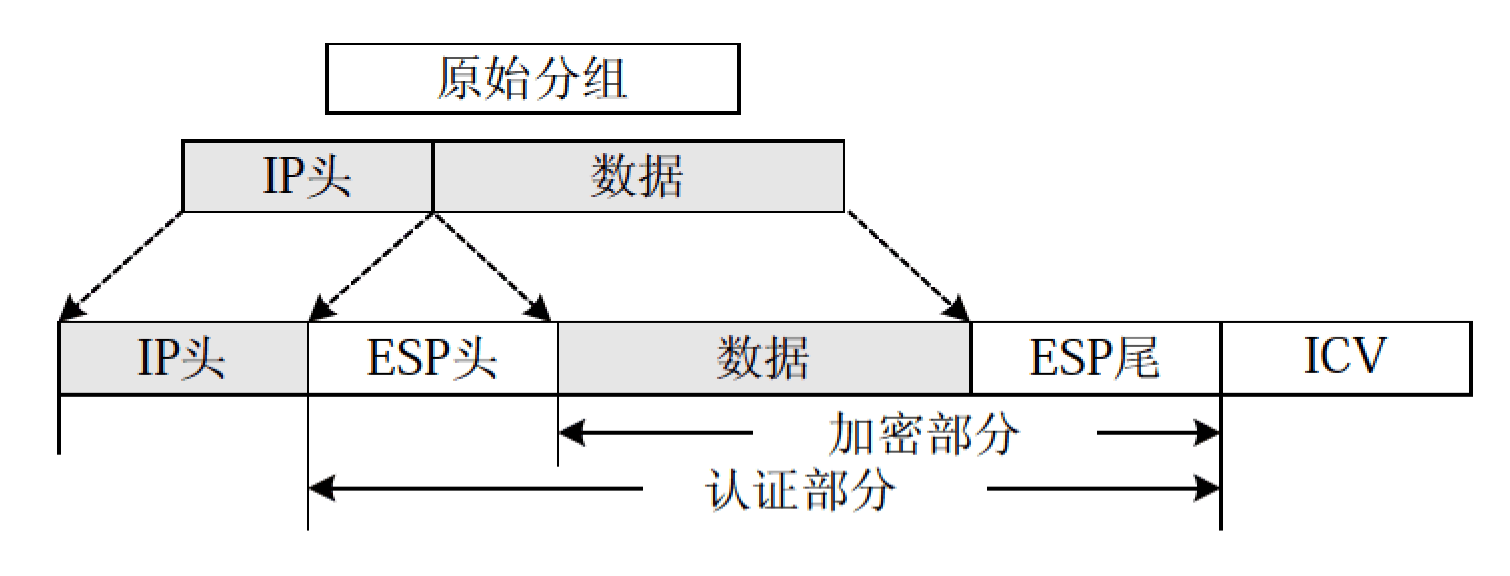


图 9-20　ESP 传输模式

2. 隧道模式

在数据包最终目的地不是安全终点的情况下，通常需要在隧道模式下使用 IPSec。假如安全保护能力需要由一个设备提供，而该设备并非数据包的始发点；或者数据包需要保密传送到实际目的地不同的另一个目的地，便需要采用隧道模式。例如，当一台主机为了获得对某个网关控制的网络的访问而与这些网关中的某一个建立连接时，就可以使用 IPSec 隧道模式。

在隧道模式中，不是将原始的 IP 协议头移到最左边然后插入 IPSec 协议头，而是复制原始 IP 协议头，并将复制的 IP 协议头移到数据报最左边作为新的 IP 协议头。随后，在原始 IP 协议头与 IP 协议头的副本之间放置 IPSec 协议头。原始 IP 协议头保持原封不动，并且整个原始 IP 协议头都被认证或由加密算法进行保护。也就是说，IPSec 隧道模式的数据库包有两个 IP 头，即内部 IP 头和外部 IP 头。其中，内部头由主机创建，而外部头是由提供安全服务的那个设备添加的。

在隧道模式下，整个原数据包被当作有效载荷封装了起来，外面附上新的 IP 报头。其中“内部”IP 报头（原 IP 报头）指定最终的信源和信宿地址，而“外部”IP 报头（新 IP 报头）中包含的常常是作中间处理的安全网关地址。

与传输模式不同，在隧道模式中，原 IP 地址被当作有效载荷的一部分受到 IPSec 的安全保护；另外，通过对数据加密，还可以将数据包目的地址隐藏起来，这样更有助于保护端到端隧道通信中数据的安全性。

ESP 隧道模式中签名部分（完整性检查和认证部分）和加密部分如图 9-21 所示。ESP 的签名不包括新 IP 头。

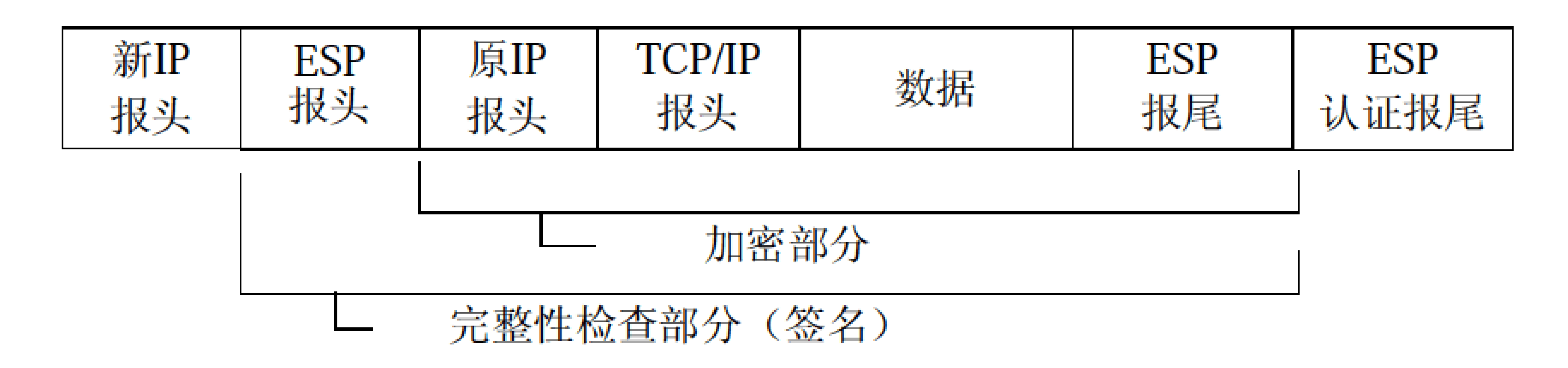


图 9-21　ESP 隧道模式



图 9-22 标示出了 AH 隧道模式中的签名部分。AH 隧道模式为整个数据包提供完整性检查和认证，认证功能优于 ESP。但在隧道技术中，AH 协议很少单独实现，通常与 ESP 协议组合使用。

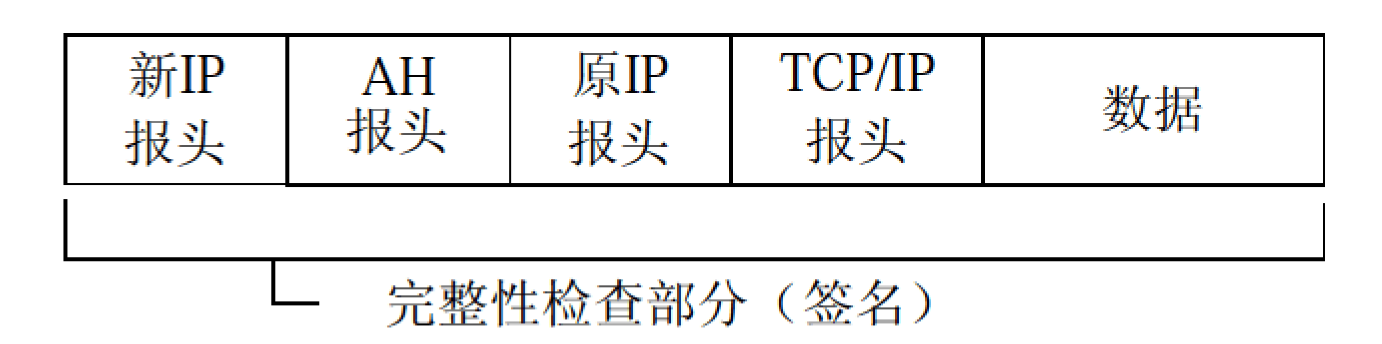


图 9-22　AH 隧道模式

9.7.4　认证报头

认证报头 AH 可为 IP 通信提供无连接的数据源认证、数据完整性和反重播保障，保护通信免受篡改，但不能防止窃听，适用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报头，此报头包含一个带密钥的 Hash 散列（可以将其当作数字签名，只是它不使用证书），此 Hash 散列在整个数据包中计算，因此对数据的任何更改将致使散列无效，这样就提供了完整性保护。

AH 报头的位置在 IP 报头和传输层协议报头之间，如图 9-23 所示。认证报头包括认证数据和一个序列号，共同用来验证发送方身份，确保数据在传输过程中没有被改动，防止受到第三方的攻击。IPSec 认证报头不提供数据加密，信息将以明文方式发送。AH 可以单独使用，也可以与 ESP 协议结合使用。

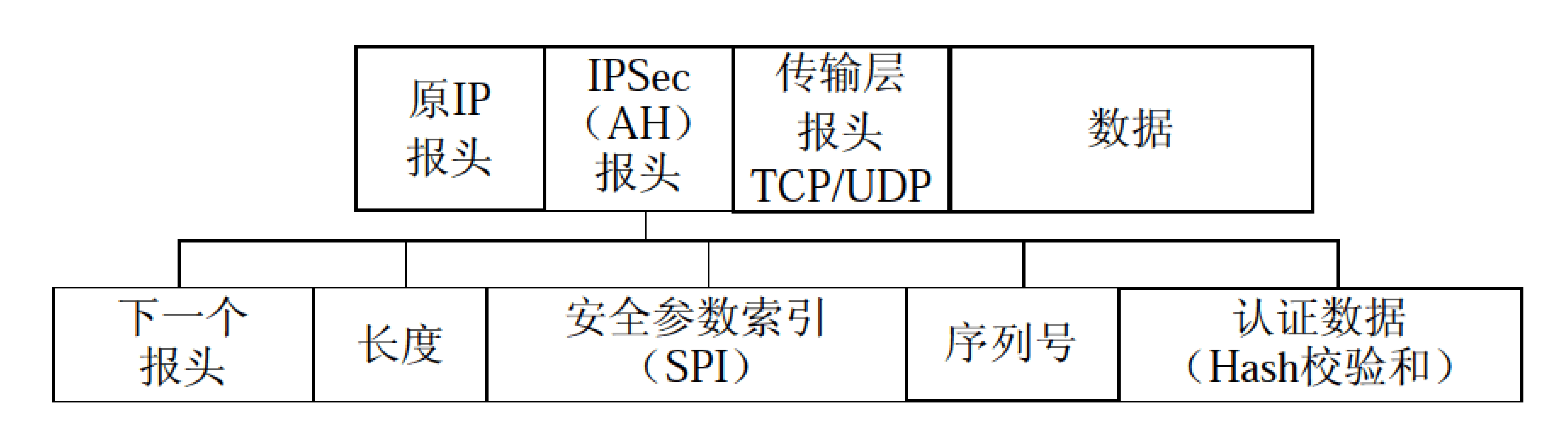


图 9-23　AH 报头

AH 报头插在 IP 报头之后，TCP、UDP 或者 ICMP 等上层协议报头之前，一般 AH 为整个数据包提供完整性检查。

9.7.5　封装有效载荷

封装有效载荷 ESP 协议主要用来处理对 IP 数据包的加密，对认证也提供某种程度的支持。也就是说，ESP 为 IP 数据包提供完整性检查、认证和加密，可以看作是“超级 AH”，因为它提供了机密性并可防止篡改。

ESP 的加密服务是可选的，但如果启用加密，则也就同时选择了完整性检查和认证。因为如果仅使用加密，入侵者就可能伪造包以发动密码分析攻击。

ESP 可以单独使用，也可以和 AH 结合使用。一般 ESP 不对整个数据包加密，而是只加密 IP 包的有效载荷部分，不包括 IP 头。但在端到端的隧道通信中，ESP 需要对整个数据包加密。

如图 9-24 所示，ESP 报头插在 IP 报头之后，TCP 或 UDP 等传输层协议报头之前。

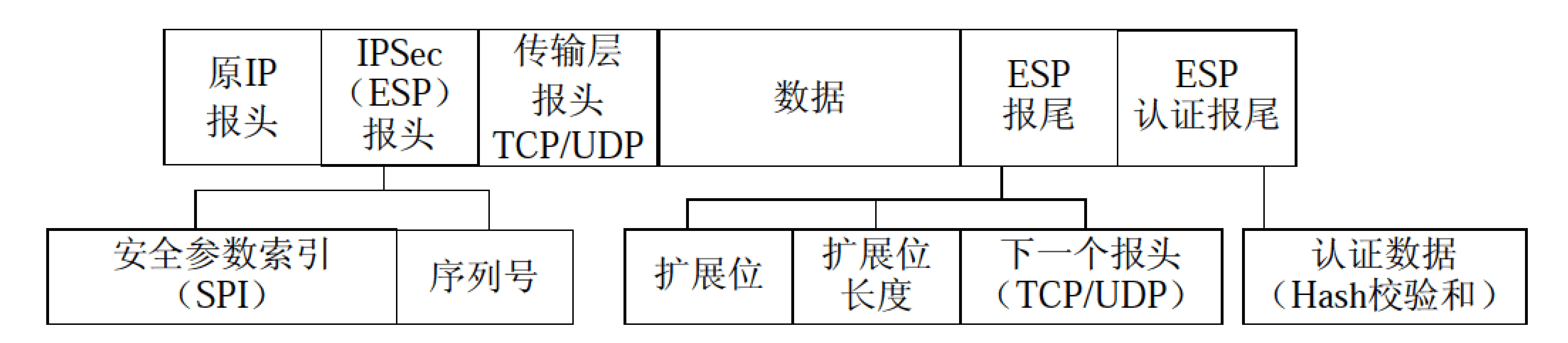


图 9-24　ESP 报头、报尾和认证报尾

9.7.6　IPSec 安全关联的建立

1. Internet 密钥交换 IKE

两台 IPSec 计算机在交换数据之前，必须首先建立某种约定，这种约定被称为“安全关联”（指双方需要就如何保护信息、交换信息等公用的安全设置达成一致，更重要的是，必须有一种方法，使那两台计算机安全地交换一套密钥，以便在它们的连接中使用）。Internet 密钥交换如图 9-25 所示。



图 9-25　Internet 密钥交换

Internet 工程任务组 IETF 制定的安全关联标准和密钥交换解决方案 IKE 负责提供一种方法供两台计算机建立安全关联 SA。SA 对两台计算机之间的策略协议进行编码，指定它们将使用哪些算法和什么样的密钥长度以及实际的密钥本身。

IKE 主要起到两个作用：安全关联的集中化管理；减少连接时间和密钥的生成及管理。

2. 建立 SA

IKE 建立 SA 分两个阶段：第一阶段，协商创建一个通信信道 IKE SA，并对该信道进行认证，为双方进一步的 IKE 通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的 IKE SA 建立 IPSec SA。分两个阶段来完成这些服务，有助于提高密钥交换的速度。

第一阶段协商（主模式协商）步骤如下。

（1）策略协商

在这一步中，就 4 个强制性参数值进行协商。

① 加密算法：选择 DES 或 3DES。

② hash 算法：选择 MD5 或 SHA。

③ 认证方法：选择证书认证、预置共享密钥认证或 Kerberos V5 认证。

④ Diffie-Hellman 组的选择。

（2）DH 交换

虽然名为“密钥交换”，但事实上在任何时候，两台通信主机之间都不会交换真正的密钥，它们之间交换的只是一些 DH 算法生成共享密钥所需要的基本材料信息。DH 交换可以是公开的，也可以受保护。在彼此交换过密钥生成“材料”后，两端主机可以各自生成完全一样的共享“主密钥”，保护紧接其后的认证过程。

（3）认证

DH 交换需要得到进一步认证，如果认证不成功，通信将无法继续下去。“主密钥”结合在第一步中确定的协商算法，对通信实体和通信信道进行认证。在这一步中，整个待认证的实体载荷，包括实体类型、端口号和协议，均由前一步生成的“主密钥”提供机密性和完整性保证。

第二阶段协商消息受第一阶段SA的保护，任何没有第一阶段SA保护的消息将被拒收。第二阶段协商建立 IPSec SA，为数据交换提供 IPSec 服务，为数据传输建立安全关联。第二阶段协商（快速模式协商）步骤如下。

（1）策略协商

双方交换保护需求：① 使用哪种 IPSec 协议——AH 或 ESP；② 使用哪种 Hash 算法——MD5 或 SHA；③ 是否要求加密，若是，选择加密算法——3DES 或 DES。在上述 3 方面达成一致后，将建立起两个 SA，分别用于入站和出站通信。

（2）会话密钥“材料”刷新或交换

在这一步中，将生成加密 IP 数据包的“会话密钥”。生成“会话密钥”所使用的“材料”可以和生成第一阶段 SA 中“主密钥”的相同，也可以不同。如果不作特殊要求，只需要刷新“材料”后，生成新密钥即可。若要求使用不同的“材料”，则在密钥生成之前，首先进行第二轮的 DH 交换。

（3）将 SA 和密钥连同 SPI 递交给 IPSec 驱动程序，由其负责监视、筛选和保护 IP 通信

IPSec 驱动程序负责监视所有出/入站的 IP 数据包，并将每个 IP 数据包与作为 IP 策略一部分的 IP 筛选器相匹配。一旦匹配成功，IPSec 驱动程序便会通知 IKE 开始安全协商。

第二阶段协商过程与第一阶段协商过程类似，不同之处在于在第二阶段中，如果响应超时，则自动尝试重新进行第一阶段 SA 协商。

第一阶段 SA 建立起安全通信信道后保存在高速缓存中，在此基础上可以建立多个第二阶段 SA 协商，从而提高整个建立 SA 的速度。只要第一阶段 SA 不超时，就不必重复第一阶段的协商和认证。允许建立的第二阶段 SA 的个数由 IPSec 策略属性决定。

3. IPSec 的体系结构

（1）IPSec 驱动程序

IPSec 驱动程序负责监视、筛选和保护 IP 通信，可监视所有出/入站的 IP 数据包，并将每个 IP 数据包与作为 IP 策略一部分的 IP 筛选器相匹配。一旦匹配成功，IPSec 驱动程序便会通知 IKE 开始安全协商。图 9-26 为 IPSec 驱动程序服务示意图。

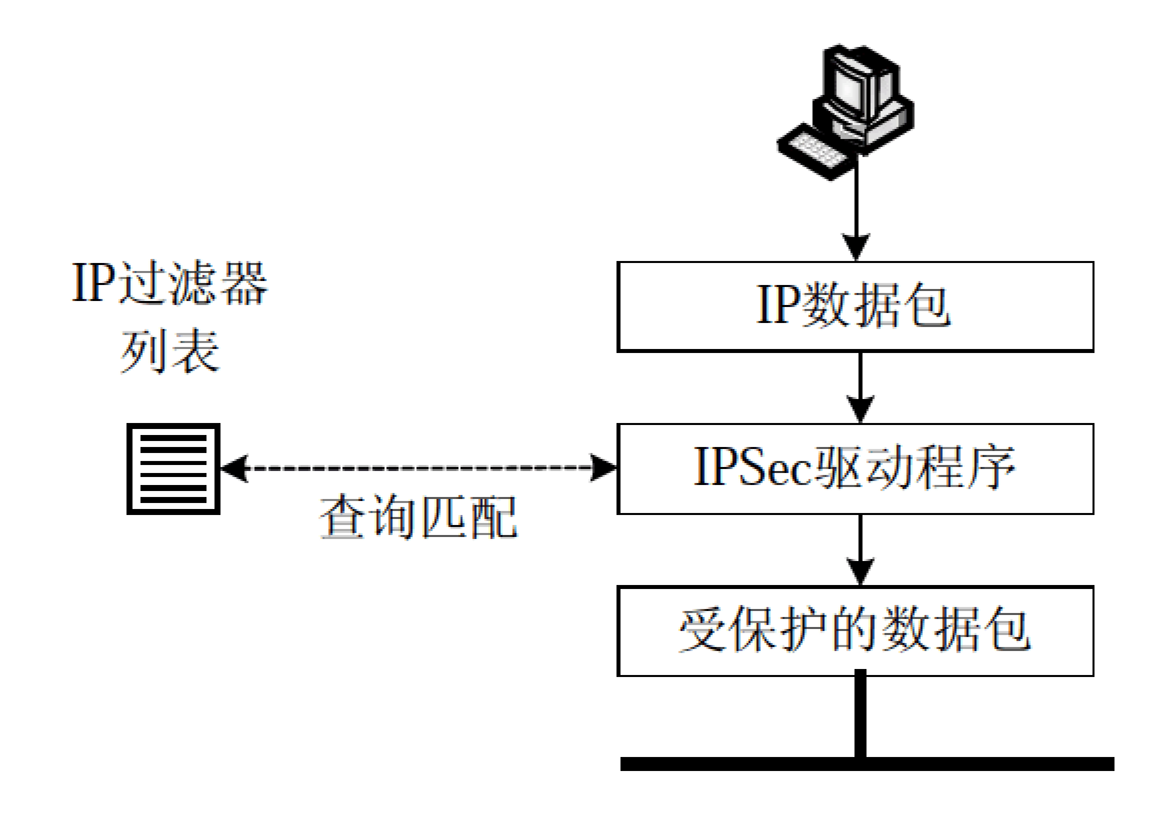


图 9-26　IPSec 驱动程序服务

在安全协商成功完成后，发送端的 IPSec 驱动程序执行以下步骤。

① 从 IKE 处获得 SA 和会话密钥。

② 在 IPSec 驱动程序数据库中查找相匹配的出站 SA，并将 SA 中的 SPI 插入 IPSec 报头。

③ 对数据包进行签名、完整性检查；如果要求加密保护，则另外加密数据包。

④ 将数据包随同 SPI 发送至 IP 层，然后进一步转发至目的主机。

接收端的 IPSec 驱动程序执行以下步骤。

① 从 IKE 处获得会话密钥、SA 和 SPI。

② 通过目的地址和 SPI 在 IPSec 驱动程序数据库中查找相匹配的入站 SA。

③ 检查签名，对数据包进行解密（如果是加密包的话）。

④ 将数据包递交给 TCP/IP 驱动程序，然后再交给接收应用程序。

（2）IPSec 体系结构模型

在分别介绍了 IKE 密钥管理和 IPSec 驱动程序后，来看一个完整的 IPSec 体系结构模型（如图 9-27 所示），以便更好地理解 IPSec 体系结构。

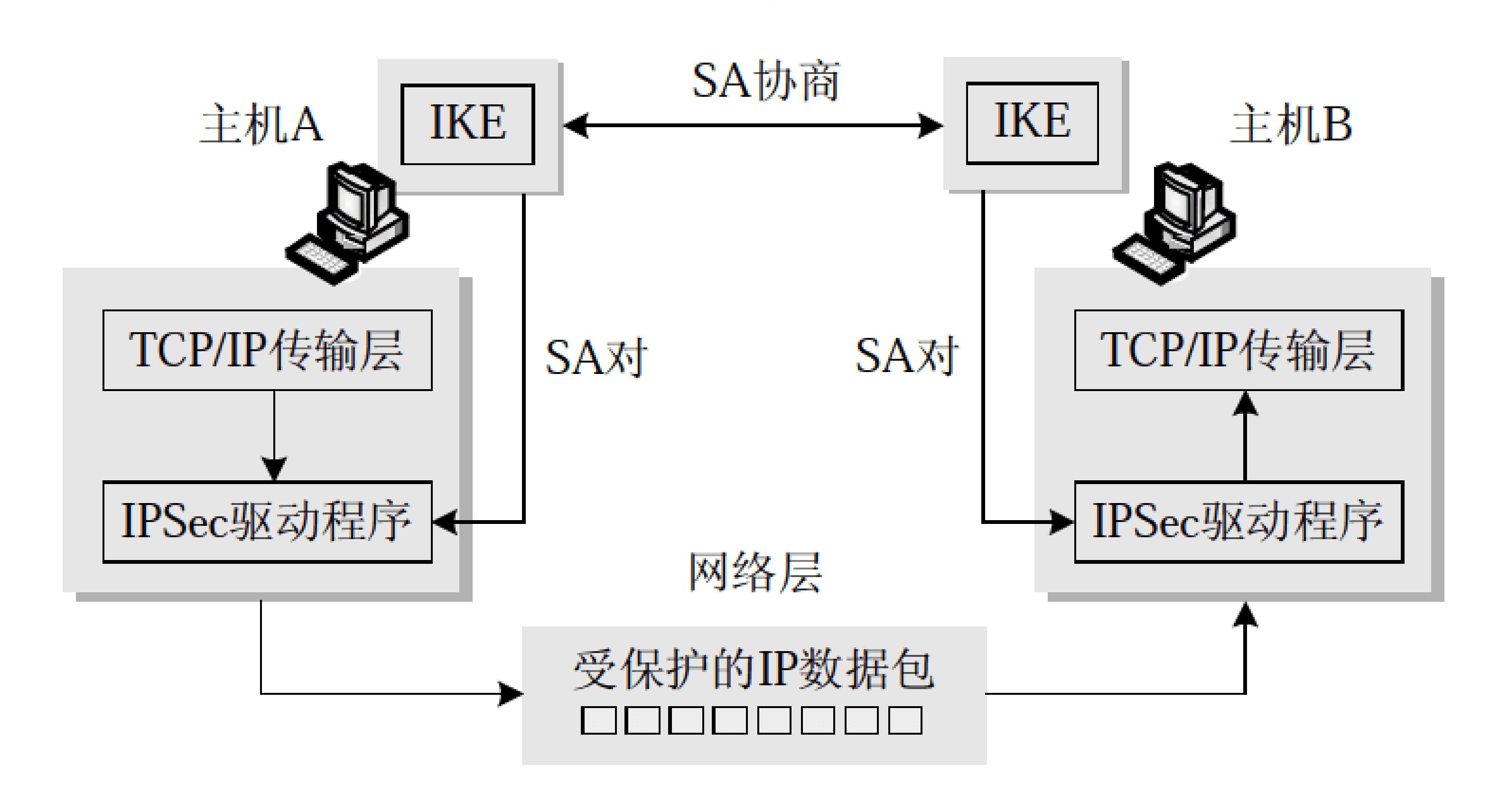


图 9-27　IPSec 流程图

为简单起见，假设这是一个 Intranet 例子，每台主机都有处于激活状态的 IPSec 策略。

① 用户甲（在主机 A 上）向用户乙（在主机 B 上）发送一个消息。

② 主机 A 上的 IPSec 驱动程序检查 IP 筛选器，查看数据包是否需要受保护以及需要受到何种保护。

③ 驱动程序通知 IKE 开始安全协商。

④ 主机 B 上的 IKE 收到请求安全协商通知。

⑤ 两台主机建立第一阶段 SA，各自生成共享“主密钥”。值得注意的是，若两机在此前通信中已经建立起第一阶段 SA，则可直接进行第二阶段 SA 协商。

⑥ 协商建立第二阶段 SA 对：入站 SA 和出站 SA。SA 包括密钥和 SPI。

⑦ 主机 A 上的 IPSec 驱动程序使用出站 SA 对数据包进行签名（完整性检查）与/或加密。

⑧ 驱动程序将数据包递交 IP 层，再由 IP 层将数据包转发至主机 B。

⑨ 主机 B 的网络适配器驱动程序收到数据包，并提交给 IPSec 驱动程序。

⑩ 主机 B 上的 IPSec 驱动程序使用入站 SA 检查完整性签名与/或对数据包进行解密。

⑪ 驱动程序将解密后的数据包提交上层 TCP/IP 驱动程序，再由 TCP/IP 驱动程序将数据包提交主机 B 的接收应用程序。

以上是 IPSec 的一个完整工作流程，虽然看起来很复杂，但所有操作对用户是完全透明的。中介路由器或转发器仅负责数据包的转发，如果中途遇到防火墙、安全路由器或代理服务器，则要求它们具有 IP 转发功能，以确保 IPSec 和 IKE 数据流不会遭到拒绝。

这里需要指出的一点是，使用 IPSec 保护的数据包不能通过网络地址译码 NAT。因为 IKE 协商中所携带的 IP 地址是不能被 NAT 改变的，对地址的任何修改都会导致完整性检查失效。

小　　结

TCP/IP 即传输控制协议/网际协议，是 Internet 上使用的一组完整的标准网络连接协议。TCP/IP 的层次不同提供的安全性也不同，例如在网络层提供虚拟专用网络，在传输层提供安全套接服务。TCP/IP 协议模型的网络安全贯穿于各个层次，即网络接口层、网际层、传输层和应用层。为此，基于 TCP/IP 分层的网络安全服务也是分层的，不同层次的网络服务是不同的，应用中需要分层进行配置。

万维网 WWW 是一个在 Internet 上运行的分布式的信息服务系统，是一个大规模、联机式的信息储藏所。它由遍布全世界的数以万计的 Web 站点组成。Web 赖以生成的环境包括计算机硬件、操作系统、计算机网络、许多的网络服务和应用，所有这些都存在着安全隐患，最终威胁到 Web 的安全。对于 Web 服务的安全性，一定要考虑到所有这些方面，因为它们是相互联系的，每个方面都会影响到 Web 服务的安全性，它们中安全性最差的决定了给定服务的安全级别。

电子商务包含两方面内容，一是电子方式，二是商贸活动。电子商务所面临威胁的出现导致了对电子商务安全的需求，也是真正实现一个安全电子商务系统所要求实现的各个

特性，主要包括机密性、完整性、认证性和不可抵赖性。

目前的网络攻击模式呈现多方位、多手段化，让人防不胜防。概括来说分为 4 大类：拒绝服务攻击、利用型攻击、信息收集型攻击、假消息攻击。

电子邮件是 Internet 上最常用的功能之一，用户可以通过 Internet 交换邮件形式的信息文件。当前电子邮件系统的发展面临着机密泄漏、信息欺骗、病毒侵扰、垃圾邮件等诸多安全问题的困扰。

虚拟专用网 VPN 是指将物理上分布在不同地点的网络通过公用网络连接而成逻辑上的虚拟子网，并采用认证、访问控制、机密性、数据完整性等在公用网络上构建专用网络的技术，使得数据通过安全的“加密隧道”在公用网络中传播。

IPSec 在 IP 层提供安全服务，使得系统能够按需选择安全协议，决定服务所使用的算法及放置需求服务所需密钥到相应位置；用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。IPSec 可提供的安全服务集包括访问控制、无连接的完整性、数据源认证、拒绝重发包（部分序列完整性形式）、保密性和有限传输流保密性。

练习与思考

1. 简述 TCP/IP 协议的层次安全。
2. 简述 Web 的安全需求。
3. 什么是电子商务？简述安全电子商务体系结构。
4. 什么是 SSL？它的结构如何？
5. 什么是 SET？简述 SET 协议的支付过程。
6. 简述网络攻击的类型和流程。
7. 电子邮件存在哪些安全威胁？如何防范？
8. 什么是 VPN？它是如何解决安全问题的？简述它的工作原理。
9. 什么是 IPSec？什么是安全关联？
10. 评价 IPSec 的两种实现机制。
11. 比较 AH 和 ESP 协议报文格式的异同。

第10章

无线网络安全

本章学习要求：

（1）掌握无线网络标准。
（2）掌握无限局域网有线等价保密机制。
（3）掌握无线局域网有线等价安全漏洞。
（4）了解无线局域网安全威胁。
（5）了解无线保护接入安全机制。

重点和难点

（1）重点：无线网络标准。
（2）难点：无线局域网有线等价保密安全机制。

采用双绞线、同轴电缆或光纤等传输介质实现数据通信的网络称为有线网络，采用无线链路实现数据通信的网络则称为无线网络。随着移动电话、个人数字助理、笔记本电脑、掌上计算机等各种便携式终端的迅速发展，为移动计算提供支撑环境、可以随时随地进行通信的无线网络日益受到重视。相对于有线网络，无线网络为用户提供便利性的同时，也为基于无线链路和智能移动终端蓄意破坏、篡改、窃听、假冒、泄露和非法访问信息资源的各种恶意行为提供了方便。因此，无线网络比有线网络存在更多的安全隐患和威胁。此外，由于无线网络本身体系结构复杂、传输速率慢、信号易受干扰、安全隐患多、通信成本高等固有的局限性，目前有线网络仍然是计算机网络的主体，无线网络只是有线网络的补充，主要用于不便布线和要求移动计算的场合。

无线网络技术是当前网络技术发展和应用的热点和重要方向，本章将对无线网络标准、无线局域网有线等价保密机制、无线局域网有线等价保密安全漏洞、无线局域网安全威胁、无线保护接入安全机制等进行综合分析。

10.1 无线网络标准

无线通信网络根据应用领域可分为蜂窝移动通信网、无线局域网、无线个人区域网和无线城域网多种类型；而随着无线通信技术的迅速发展，也出现了多种无线通信网络标准。蜂窝移动通信正在从广泛使用的全球移动通信系统、码分多址、通用分组无线业务向国际移动电信第三代移动通信标准过渡；无线局域网有 IEEE 802.11、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 和满足多媒体数据业务需求的高性能无线局域网标准；无线个人区域网包括无线家庭网和蓝牙短距离无线网标准；面向大范围覆盖的无线城域网标准 IEEE 802.16 也在逐步实施之中。

10.1.1 第二代蜂窝移动通信网

20 世纪 70 年代诞生的模拟蜂窝移动通信系统是第一代（1G）移动通信系统，采用模拟信号传输方式实现语音业务，使用频分多址（Frequency Division Multiple Address，FDMA）接入技术划分信道。由于 1G 系统存在诸如频谱利用率低、语音质量差、接入容量小、保密性差和不能提供数据通信服务等先天不足，目前已被数字蜂窝移动通信系统取代，形成了覆盖全球的第二代（2G）移动通信网。目前 2G 移动通信系统主要有全球移动通信系统（Global System for Mobile Communication，GSM）和码分多址（Code Division Multiple Access，CDMA）两大移动通信标准。

1. 全球移动通信系统 GSM 标准

1991 年欧洲电信标准协会（European Telecommunication Standard Institute，ETSI）推出了 GSM 泛欧数字蜂窝移动通信标准，不仅提供了移动电话语音服务，还提供了紧急呼叫、短消息、语音信箱、可视图文等多种数据服务。GSM 采用时分多址（Time Division Multiple Address，TDMA）窄带标准，可以分别工作在 900MHz、1800MHz 和 1900MHz 三个不同频段，其中 900MHz 频段又分为 EGSM 900MHz 和 GSM 900MHz 两个频段。EGSM 900MHz 频段的上行、下行频率分别为 880～890MHz 和 925～935MHz，GSM 900MHz 频段的上行、下行频率分别为 890～915MHz 和 935～960MHz，双工间隔为 45MHz。1800MHz 频段的上行、下行频率分别为 1710～1785MHz 和 1805～1880MHz，双工间隔为 95MHz。1900MHz 频段的上行、下行频率分别为 1850～1910MHz 和 1930～1990MHz，双工间隔为 80MHz。GSM 标准最大可提供 9.6Kbps 的数据传输速率，我国和世界上其他 170 多个国家采用 GSM 标准，其中我国、欧洲和东南亚地区都采用 900MHz 和 1800MHz 频段。GSM 900MHz 频段的频分双工频谱分配如图 10-1 所示。

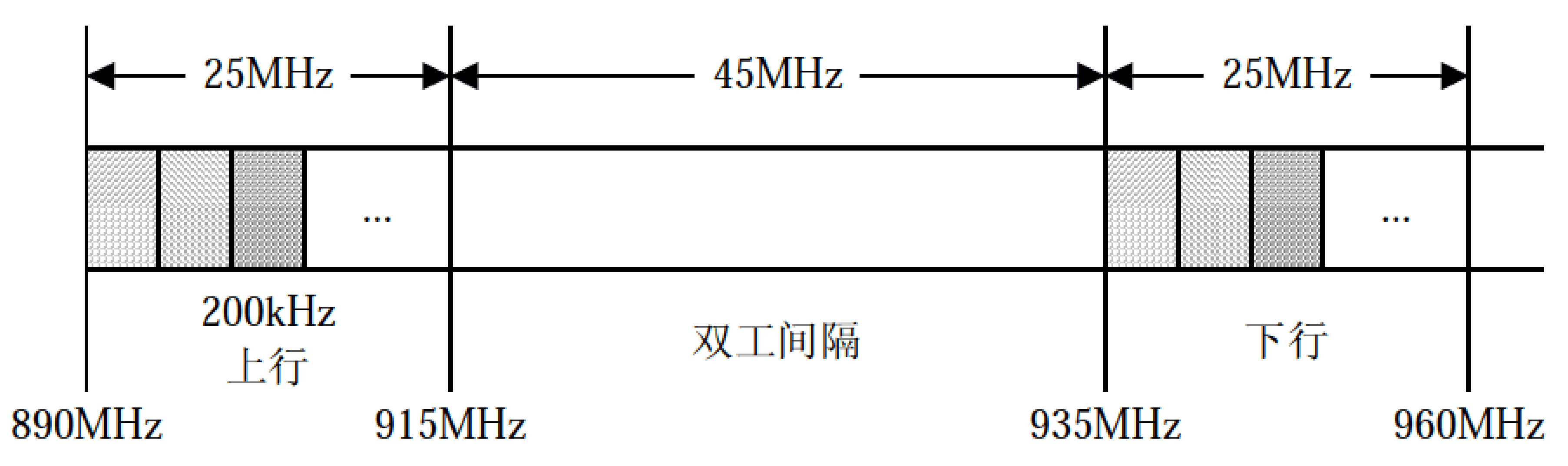


图 10-1　GSM 频分双工频谱分配

上行和下行载波频率各占用 25MHz 带宽，移动电话的接收频率比发射频率高，构成一个频分双工信道。在 25MHz 带宽内分成 124 个载波信道，每个载波信道占用 200kHz 的带宽。载波信道又分成 8 个 TDMA 时隙，每个时隙宽度为 0.578ms。时隙就是 TDMA 物理意义上的信道。

2. 码分多址 CDMA 标准

FDMA 以不同频率区分移动电话地址，其特点是频带独占，而时间资源共享；TDMA 采用不同时隙区分地址，特点是时隙独占，而频率资源共享；CDMA 则采用不同码型区分地址，特点是码型独占，而频率和时间资源共享。由于分配给移动电话的地址码型具有唯一性，CDMA 系统就能够在同一时间和同一频率下实现通信，因而拥有巨大的通信容量。如图 10-2 所示为采用频率划分前向和反向信道的 CDMA 码分信道，基站对移动电话方向为前向信道，其载波频率为 f_1，移动电话对基站方向为反向信道，载波频率为 f_2。每个移动用户分配一个地址码型 C_i，且不同地址码型 C_1、C_2、…、C_i、…、C_k 相互正交。地址码型和移动用户具有一一对应关系，因此利用地址码型就可以实现选址通信。在蜂窝移动通信系统中，为了充分利用信道资源，地址码型是由基站通过信令信道动态分配给移动用户的。

前向信道f_1	C_1	C_2	C_3	…	C_i	…	C_k
反向信道f_2	C_1	C_2	C_3	…	C_i	…	C_k

图 10-2　CDMA 频分双工码分信道

CDMA 系统采用了扩频通信（Spread Spectrum）技术，扩频通信就是扩展基带信号的频谱，其带宽通常是基带信号频带的 100～1000 倍。扩频通信具有很强的信号抗干扰能力，而且扩频信号的频谱接近白噪声，有利于信号隐蔽和通信保密。早期扩频通信主要用于军事通信，随着扩频通信技术的发展，目前已广泛用于民用移动通信。扩频通信的理论基础是下面给出的著名香农（Shannon）定理：

$$C = H\log_2\left(1 + \frac{S}{N}\right)$$

其中，C 表示信道容量或信道的极限信息传输速率，H 为信号带宽，S 是信道内信号的平均功率，N 是信道内高斯噪声功率。

香农定理说明，在保持信道信息传输速率不变的前提下，扩展信号带宽就相当于提高了信号的信噪比，增强了信号的抗干扰能力。

目前广泛使用的扩频技术主要有直序扩频（Direct Sequence Spread Spectrum，DSSS）和跳频扩频（Frequency Hopping Spread Spectrum，FHSS）。DSSS 在发送端使用伪随机码扩展信号频谱，接收端使用相同的伪随机码将扩频信号恢复成基带信号。FHSS 也使用伪随机码扩展信号频谱，但扩频方法与 DSSS 不同。FHSS 首先用伪随机码形成跳频指令，跳频指令控制载波频率在跳频带宽内随机跳变，达到扩展信号频谱的目的。

美国 Qualcomm 公司提出的 Q-CDMA 是世界上第一个商用 CDMA 数字蜂窝移动通信系统，后经美国电信工业协会批准成为 CDMA/IS-95 标准。其前向信道、反向信道的频段分别为 869～894MHz 和 824～949MHz，载波间隔为 1.25MHz，最大可提供 9.6Kbps 的数据传输速率。

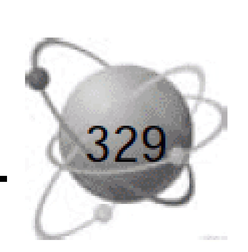
10.1.2 通用分组无线业务网

GSM 和 CDMA 都是典型的电路交换数字蜂窝移动通信标准，随着 Internet 的迅速发展，基于 IP 分组交换的数据传输必然成为无线通信的发展目标。但 IP 移动通信需要一个逐步成熟的过程，为此诞生了过渡阶段的 2.5G 移动通信标准。欧洲电信标准协会提出的通用分组无线业务（General Packet Radio Service，GPRS）是典型的 2.5G 移动通信标准之一，采用分组交换传输模式，以语音通信为主，数据通信为辅，最大可提供 171.2Kbps 的数据传输速率。

GPRS 是在 GSM 移动通信系统的基础上提供的分组无线业务标准，是 GSM 迈向 3G 的重要步骤。GPRS 与 GSM 具有相同的频段、双工间隔、频带宽度、载频间隔和 TDMA 帧结构，但现有的 GSM 移动终端不能直接在 GPRS 中使用。由于采用了分组交换技术，用户只在数据通信期间占用信道资源，在提高信道资源利用率的同时，也为按通信数据量、业务类型和服务质量计费奠定了基础。GPRS 支持 Internet 上应用广泛的 IP 协议和 X.25 协议，能够无线接入 Internet 和其他分组网络。目前世界上已有近百个移动运营商开通了 GPRS 商用系统，中国移动通信集团公司也于 2002 年 5 月 17 日正式推出了 GPRS 商用服务。

10.1.3 第三代蜂窝移动通信网

国际电信联盟（International Telecommunication Union，ITU）早在 1985 年就提出了第三代（3G）移动通信的雏形，当时称为未来公众陆地移动电信系统（Future Public Land Mobile Telecommunication Systems，FPLMTS），1996 年 ITU 将其正式更名为国际移动电信-2000（International Mobile Telecommunication-2000，IMT-2000），隐含的意义是 3G 移动通信工作在 2000MHz 频段并于 2000 年实现商用。尽管 GSM 和 CDMA 形成了全球 2G 移动通信的主流标准，但不同国家和运营商使用的标准和频段仍然有很大差异，很难实现移动用户的全球漫游。有鉴于此，IMT-2000 希望在全球范围内统一标准和频段，为实现全球无缝漫游消除障碍；在提高频谱利用率的同时，提供文本、语音、音乐、图像、视频等多媒体移动通信服务，并根据不同移动用户的需求，分别支持 2Mbps、384Kbps 和 144Kbps 的数据



传输速率。当移动速度小于 10km/h 时，提供 2Mbps 的数据传输速率；小于 120km/h 时，提供 384Kbps 的速率；大于 120km/h 时，能够支持 144Kbps 的速率。由此可以看出，统一标准和频段、提高频谱利用率和支持多媒体移动通信正是 3G 移动通信与 2G 的主要区别。

由于移动通信标准直接影响国家、运营商和移动终端生产厂商的经济利益，ITU 在协调多方利益的基础上，于 2000 年 5 月从 10 个 3G 移动通信候选方案中确定了 5 个推荐标准，其中欧洲提出的宽带 WCDMA（Wideband CDMA）、美国提出的 CDMA2000 和中国制定的时分同步 TD-SCDMA（Time Division-Synchronous CDMA）最有可能成为未来 3G 移动通信的主流标准。其中 WCDMA 和 CDMA2000 采用频分双工（Frequency Division Duplex，FDD）信道，TD-SCDMA 采用时分双工（Time Division Duplex，TDD）信道。

WCDMA 的支持者主要是欧洲、日本等国家的 GSM 网络运营商和生产厂商，能够在现有 GSM 网络基础上，途经 GPRS 逐步过渡到 3G 移动通信。CDMA2000 是在 CDMA/IS-95 基础上制定的标准系列，包括 CDMA2000 1X、CDMA2000 1X EV-DO、CDMA2000 1X EV-DV 和 CDMA2000 3X 多个子标准，计划分多个阶段逐步实施，北美洲国家、韩国、日本等国的 CDMA 网络运营商和生产厂商是其主要支持者。CDMA2000 1X 为第一过渡阶段，在 CDMA/IS-95 基础上引入了分组交换技术，能够支持移动 IP 业务，最大数据传输速率为 308Kbps。类似于 GSM 系统中的 GPRS，多数人将 CDMA2000 1X 归类到 2.5G 移动通信。CDMA2000 1X EV-DO 和 CDMA2000 1X EV-DV 是 CDMA2000 1X 的演变升级体制，其中 EV 就是英文 Evolution 的缩写。CDMA2000 1X EV-DO（Data Only）采用专用数据信道传输数据，目的就是要提高数据传输速率，最大数据传输速率可达 2.4Mbps。CDMA2000 1X EV-DV（Data and Voice）采用数据信道和语音信道共享方式，在提高接入容量的同时，将最大数据传输速率提高到 3.1Mbps。CDMA2000 3X 是 CDMA2000 的第二过渡阶段，同 CDMA2000 1X 的主要区别就是前向信道采用 3 载波方式，而 CDMA2000 1X 采用单载波方式，多载波方式能够提供更高的数据传输速率。TD-SCDMA 是中国首次经 ITU 获准的移动通信技术标准，最大数据传输速率为 2Mbps。由于中国具有庞大的移动通信市场，目前世界上已有多家电信设备厂商宣布支持 TD-SCDMA 标准。

根据 ITU 在 2004 年 12 月的统计，2004 年全球移动通信用户总数已超过 15 亿，WCDMA 和 CDMA2000 1X EV-DO 第三代移动通信用户总数已超过 2000 万。根据我国信息产业部（现已更名为中华人民共和国工业和信息化部）2004 年的统计，仅 2004 年就新增移动通信用户 6400 万，移动用户总数达到 3.34824 亿。

10.1.4 IEEE 802.11 无线局域网

能够在有限范围内实现无线通信的网络称为无线局域网（Wireless Local Area Network，WLAN）。WLAN 分为有固定基础设施和无固定基础设施两类，固定基础设施指预先建立的基站或接入点（Access Point，AP），主要用于将无线客户端接入有线网络，AP 网络节点用于桥接有线网络和 WLAN。在有固定基础设施模式下，WLAN 的最小构件称为基本服务集（Basic Service Set，BSS），无线客户端与其他无线客户端及有线网络主机之间的通信需

要 AP 转发，才能发送到目的端。基本服务集可以是孤立的，也可以通过分布式系统接入其他基本服务集，通过分布式系统互联起来的 WLAN 称为扩展服务集（Extended Service Set，ESS），扩展服务集在逻辑上相当于一个基本服务集。

无固定基础设施指没有安装 AP 的 WLAN，其最小构件称为独立基本服务集（Independent Basic Service Set，IBSS）。没有预先设置 AP 的 WLAN 也称为自组网络（Ad Hoc Network）或对等网络（Peer-Peer Network），主要用于无线客户端之间的通信，一般不与外界的其他网络互联。自组网络最多容许 9 个无线客户端。有固定基础设施和无固定基础设施的 WLAN 分别如图 10-3 和图 10-4 所示。

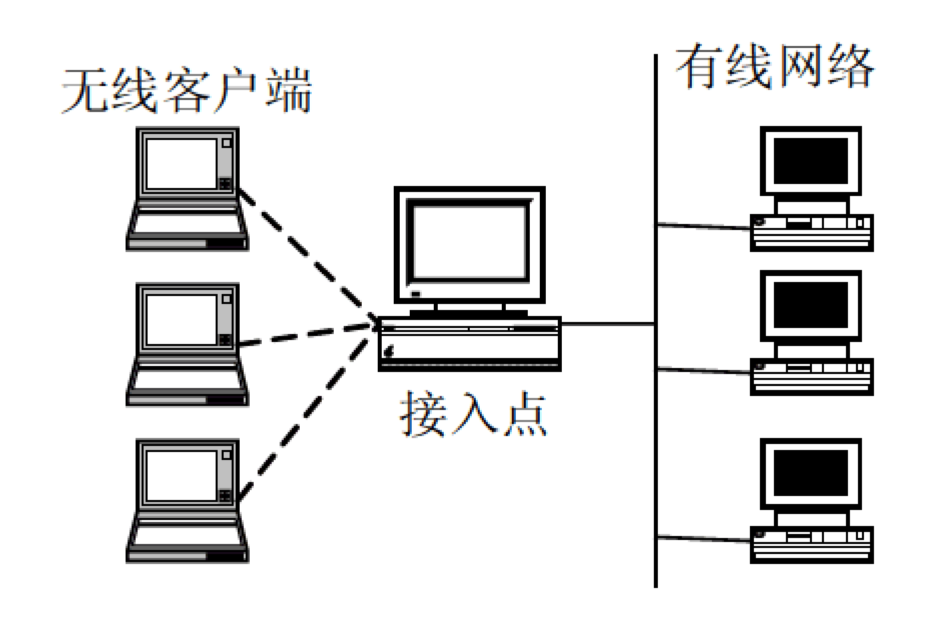


图 10-3 有固定基础设施的 WLAN

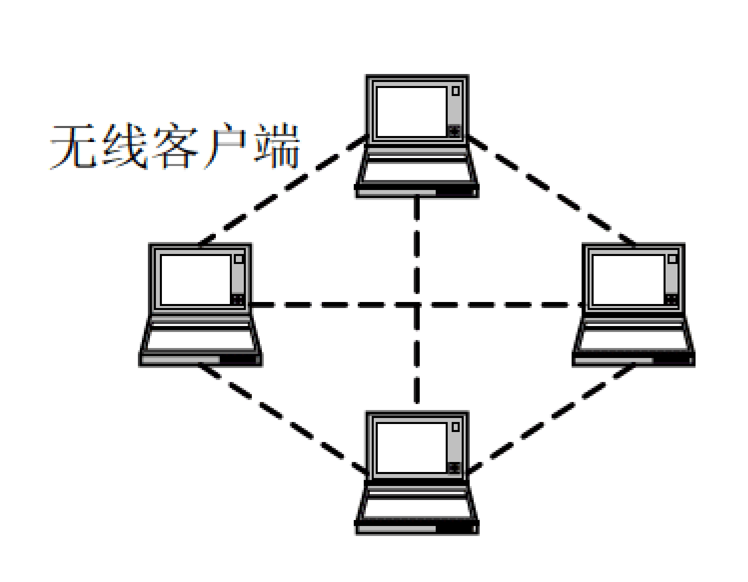


图 10-4 自组 WLAN

国际电气和电子工程师学会早在 1997 年就发布了 IEEE 802.11 无线局域网标准，规范了 WLAN 的 MAC 层协议和物理层规程，使不同厂商生产的无线设备能够实现无线互联。IEEE 802.11 在参考 IEEE 802.3 有线以太局域网 MAC 层 CSMA/CD 协议的基础上，采用载波监听多路访问/冲突避免 CSMA/CA 协议解决多用户共享无线信道的冲突问题。物理层规程定义了跳频扩频 FHSS、直序扩频 DSSS 和红外线 IR（Infrared）3 种调制技术实现方法，并规定工作频段为不需要许可证的 2.4GHz 工业、科学和医疗 ISM（Industry Science and Medical）频段，其频段宽度为 2.4～2.4835GHz。当使用 FHSS 或 DSSS 扩频技术时，传输距离在 100m 范围内，数据传输速率可达到 1Mbps 或 2Mbps。红外线不能穿越障碍物，因此红外线调制主要用于室内通信，其波长为 850～950nm，传输速率也为 1Mbps 或 2Mbps。

为了进一步提高 WLAN 的数据传输速率，IEEE 802.11 委员会于 1999 年 7 月又发布了 IEEE 802.11a 和 IEEE 802.11b 两个标准，MAC 层协议与 IEEE 802.11 基本相同，但采用了不同的物理层规程。IEEE 802.11a 物理层使用 5GHz ISM 频段和正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）多载波调制技术，可分别支持 6、9、12、18、24、36、48、56Mbps 多种传输速率，通信距离长达 10km，能够满足不同移动用户的需求。事实上，IEEE 802.11a 采用 OFDM 多载波调制技术的目的是为了能够与 ETSI 提出的高性能无线局域网 HiperLAN 兼容。

IEEE 802.11b 物理层仍然使用 2.4GHz ISM 频段，但采用高速率直序扩频（High Rate Direct Sequence Spread Spectrum，HR-DSSS）调制技术，能够根据通信环境质量在 1、2、5.5、11Mbps 范围内自动调整传输速率，在室内有障碍的条件下最大传输距离可达 100m，室外直线传播最大传输距离可以达到 300m。IEEE 标准委员会随后在 2003 年 6 月又正式批

准了 IEEE 802.11g WLAN 标准。IEEE 802.11g 沿用了 IEEE 802.11、IEEE 802.11b 的 2.4～2.4835GHz ISM 频段，但使用 IEEE 802.11a 的 OFDM 调制扩频技术。IEEE 802.11g 完全兼容目前广泛使用的 IEEE 802.11b 技术标准，并且以低廉的成本将最大数据传输速率提高到 56Mbps；不仅支持 IEEE 802.1la 具有的 6、9、12、18、24、36、48、56Mbps 多种传输速率，也支持 IEEE 802.11b 具有的 1、2、5.5、11Mbps 传输速率；由于向下兼容 IEEE 802.11b 标准，能够在 IEEE 802.11g 和 IEEE 802.11b 标准之间自由切换。虽然 IEEE 802.11a 具有传输速率高和覆盖范围大的优点，但由于不兼容 IEEE 802.11b 标准，而且无线设备造价较高，显然 IEEE 802.11g 标准比 IEEE 802.11a 具有更好的市场前景。

因为 IEEE 并不负责测试 IEEE 802.11 标准系列无线设备的兼容性，为了解决无线产品的互操作性问题，生产厂商自发成立了全球无线以太网兼容性联盟（Wireless Ethernet compatibility alliance，WECA），后更名为无线高保真（Wireless Fidelity alliance，Wi-Fi）联盟（http://www.Wi-Fi.org）。凡通过 Wi-Fi 联盟认证的 IEEE 802.11a、IEEE 802.11b 和 IEEE 802.1lg 无线产品，准予标记 Wi-Fi CERTIFIED 兼容性标准指示图标（Standard Indicator Icons，SII）认证标签，两种不同形状的 Wi-Fi 联盟兼容性标准指示图标如图 10-5 所示。自 2000 年 3 月 Wi-Fi 联盟开始推行产品认证以来，目前已有 1500 项以上的产品获得 Wi-Fi 兼容性认证。





图 10-5　Wi-Fi 联盟兼容性标准指示图标

10.1.5　HiperLAN/2 高性能无线局域网

高性能无线局域网（High performance radio Local Area Network，HiperLAN）是 ETSI 制定的宽带无线接入网（Broadband Radio Access Networks，BRAN）计划的重要组成部分。BRAN 包括 HiperLAN/1、HiperLAN/2、HiperAccess 和 HiperLink 4 个标准，其中 HiperLAN/1 和 HiperLAN/2 用于高速 WLAN 接入，HiperAccess 用于室外远距离有线通信网络高速接入，HiperLink 提供 HiperAccess 和 HiperLAN/2 之间的近距离高速无线连接。ETSI 早在 1992 年就提出了 HiperLAN/1 WLAN 标准，由于实现成本高于随后推出的 IEEE 802.11b 标准，没有获得商业应用。2000 年 4 月 ETSI 又公布了 HiperLAN/2 标准，由欧洲、北美洲和日本等的通信厂商组成的 HiperLAN/2 全球论坛（HiperLAN/2 Global Forum，H2GF）业界组织正在积极推广 HiperLAN/2 的市场应用，目前国际上已有 50 家著名通信厂商表示支持 HiperLAN/2 标准。

HiperLAN/2 类似 IEEE 802.1la 标准，物理层使用 5GHz ISM 频段和正交频分复用 OFDM 多载波调制技术，可分别支持 6、9、12、18、27、36、54Mbps 多种传输速率，室内通信距离为 30m，室外通信距离可达 150m。IEEE 802.11、IEEE 802.11a 和 IEEE 802.11b 标准采用无连接传输方式，不能提供任何服务质量 QoS 保障；而 HiperLAN/2 采用了面向连接的传输方式，为支持多媒体数据传输服务奠定了良好的基础。面向连接有利于实现 QoS 保障，可以为每个连接分配指定的 QoS 参数（QoS 参数包括网络吞吐量、传输延迟时间、延时抖

动和数据传输误码率)。因此，HiperLAN/2 能够更好地满足多媒体数据业务的需求。

10.1.6 HomeRF 无线家庭网

HomeRF（Home Radio Frequency）是面向家庭的无线网络标准，主要用于个人计算机和家用电子设备之间的无线通信；1998 年由英特尔（Intel）、IBM、康柏（Compaq）、3COM、飞利浦（Philips）、微软、摩托罗拉（Motorola）等公司组成 HomeRF 工作组开发，随后美国联邦通信委员会（Federal Communications Commission，FCC）正式批准其为工业标准。

HomeRF 的核心技术是共享无线访问协议（Shared Wireless Access Protocol，SWAP），数据通信采用了简化的 IEEE 802.11 标准，沿用了 MAC 层 CSMA/CA 协议来获取信道的控制权，物理层仍然采用跳频扩频 FHSS 技术。语音通信采用 ETSI 制定的数字增强无绳电话（Digital Enhanced Cordless Telephony，DECT）标准。DECT 支持电路交换和分组交换两种方式，电路交换用于语音传输，分组交换用于数据传输，使用 TDMA/TDD 划分双工信道。HomeRF 1.0 支持 1.6Mbps 的数据传输速率，工作频段为 2.4GHz ISM。HomeRF 2.0 的数据传输速率则提高到 10Mbps，工作频段为 5GHz ISM。HomeRF 曾经在短距离无线网市场具有很高的占有率，但由于技术标准未公开和技术升级进展缓慢，多数公司转向支持 IEEE 802.11b 和蓝牙标准，目前已逐渐退出无线网络市场。

10.1.7 蓝牙短距离无线网

世界著名的电信设备制造商瑞典爱立信（Ericsson）公司早在 1994 年就提出了蓝牙（Bluetooth）短距离无线网技术；1998 年瑞典爱立信、芬兰诺基亚（Nokia）、日本东芝（Toshiba）、美国 IBM 和 Intel 5 家公司成立了蓝牙特别兴趣小组 SIG（Bluetooth Special Interest Group）；随后微软、3COM、朗讯、摩托罗拉、AMD、康柏、戴尔、惠普、德州仪器、飞利浦、三星、LG、夏普等许多世界著名计算机、通信及消费电子产品公司纷纷加盟 SIG 组织，希望能够在全球范围内推广蓝牙技术。截至 2004 年底，世界上已有 3000 多家公司加盟 SIG 组织，其总部位于美国堪萨斯州欧弗兰公园（Overland Park Kansas）。

1999 年 12 月 SIG 发布 Bluetooth 1.0 版本，2001 年 3 月又发布了 Bluetooth 1.1 版本规范。由于蓝牙技术获得世界上众多著名公司的支持，2002 年 3 月 IEEE 正式批准 Bluetooth 1.1 版本为 IEEE 802.15.1 标准，并将蓝牙更名为无线个人区域网（Wireless Personal Area Network，WPAN）标准，为蓝牙短距离无线网的进一步普及铺平了道路。IEEE 802.15.1 标准类似于 HomeRF，工作频段为 2.4GHz ISM，同样采用了跳频扩频技术，最大数据传输速率为 1Mbps，理想传输距离为 10cm～10m，提高发射功率后可延长到 100m。2004 年 SIG 又推出 Bluetooth 2.0 版本规范，其核心是增强数据率（Enhanced Data Rate，EDR）技术。Bluetooth 2.0 在降低功耗的同时，将 1Mbps 的数据传输速率提升到 3Mbps。

10.1.8　IEEE 802.16 无线城域网

IEEE 针对无线市场需求提出了一系列具有互补性的无线网络标准，IEEE 802.11 标准系列是面向无线局域网的标准，IEEE 802.15 标准系列是面向无线个人区域网的标准，而 IEEE 802.16 标准系列则是面向大范围覆盖的无线城域网（Wireless Metropolitan Area Network，WMAN）标准。IEEE 802.16 标准的正式名称是固定宽带无线接入系统空中接口（Air Interface for Fixed Broadband Wireless Access Systyem，AIFBWAS），而多数人更喜欢将其称为 WMAN 或无线本地回路（Wire-less Local Loop，WLL）。早在 1999 年 IEEE 就成立了 IEEE 802.16 工作组专门研究宽带固定无线接入技术标准，目的是希望能够建立全球统一的宽带无线接入标准。类似于 IEEE 802.11b Wi-Fi 和 IEEE 802.15 SIG 联盟，支持 IEEE 802.16 标准的生产厂商于 2001 年 4 月也自发成立了微波接入全球互操作性（World-wide interoperability for Microwave Access，WiMAX）联盟，旨在全球范围推广 IEEE 802.16 标准并加快市场化进程。IEEE 802.15、IEEE 802.11 和 IEEE 802.16 无线通信标准的典型应用如图 10.6 所示。

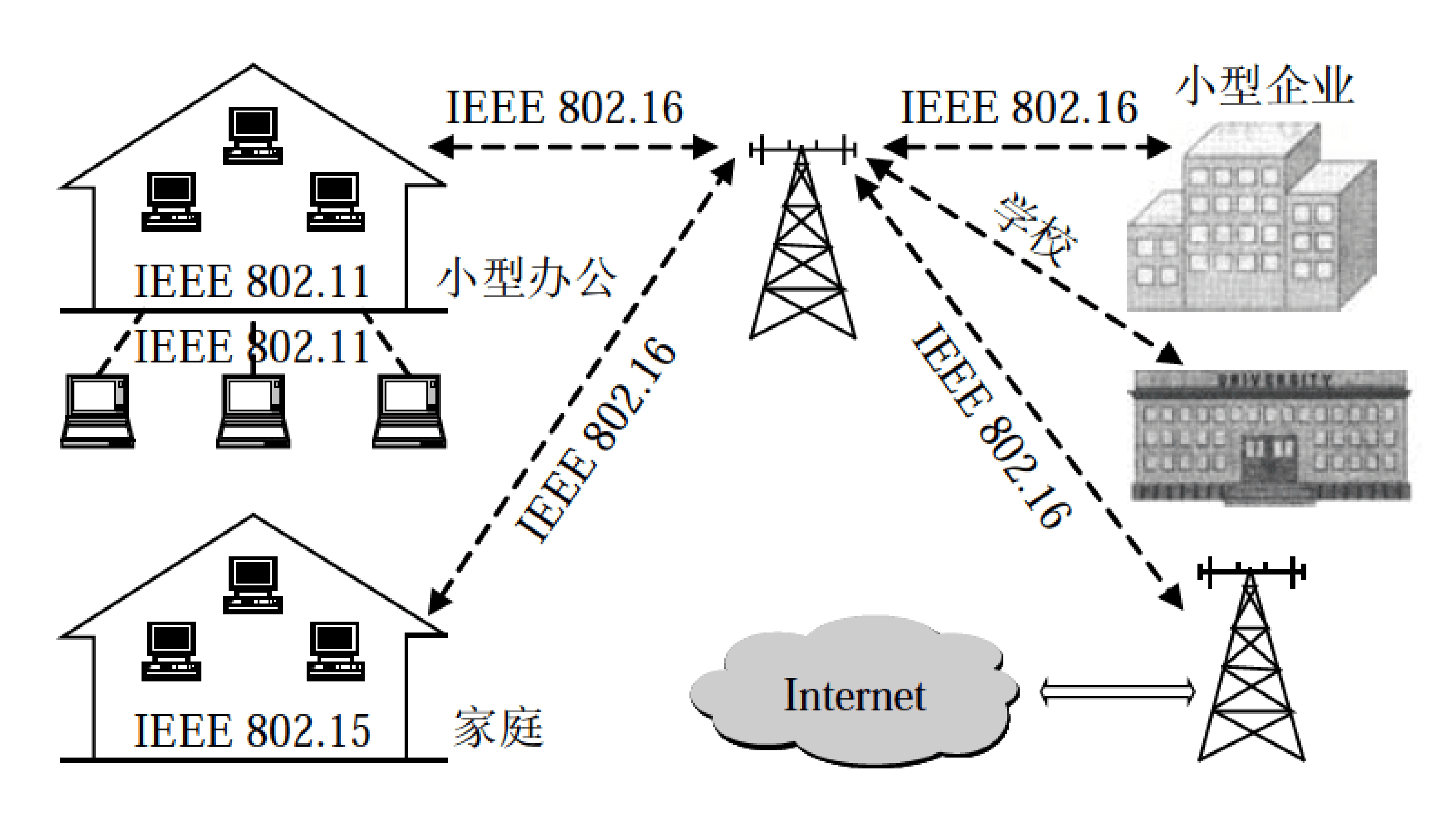


图 10-6　IEEE 802.16 WMAN 典型应用

截至目前，IEEE 802.16 WMAN 标准系列共包括 802.16、802.16a、802.16c、802.16d、802.16e、802.16f 和 802.16g 七个子标准，其中 802.16、802.16a、802.16c、802.16d 已正式发布，其余标准仍在制定和发展中。IEEE 802.16 标准系列根据是否支持移动特性分为宽带固定无线接入和移动无线接入两类。802.16、802.16a、802.16c 和 802.16d 属于宽带固定无线接入标准，802.16e 属于宽带移动无线接入标准，802.16f 是宽带固定无线接入空中接口管理信息库规范，802.16g 则是宽带固定和移动无线接入空中接口管理服务规范。

IEEE 802.16 标准对使用 2～66GHz 频段的宽带固定无线接入空中接口物理层和 MAC 层进行了规范，最大覆盖范围可达 50km。IEEE 802.16a 和 802.16c 对 IEEE 802.16 进行了扩展，分别规范了 2～11GHz 和 10～66GHz 频段的宽带固定无线接入空中接口。IEEE 802.16d 对先前颁布的标准进行了整合，将频段范围扩展成 2～66GHz。目前 IEEE 802.16 工作组已将工作重点转向宽带移动无线接入标准。

10.2 无线局域网有线等价保密安全机制

有线等价保密（Wired Equivalent Privacy，WEP）是 IEEE 802.11、802.1la、802.11b 和 802.11g 无线局域网采用的安全保护机制，IEEE 802.11 工作组希望 WEP 能够提供同有线网络完全等价的个人隐私保护。只要正确配置 WEP 的全部安全功能，WEP 仍然能够为 WLAN 应用提供基本的保密性和完整性。WEP 加密利用共享密钥在提供数据传输保密性的同时，也提供了身份认证机制，能够在一定程度上防止通过无线链路泄露、窃听和非法访问等恶意行为。通过在每帧数据中加入完整性校验值，可以提高数据在传输过程中保持完整性的能力。

10.2.1 有线等价保密 WEP

WEP 主要提供了数据加密和身份认证保护功能。数据加密采用著名密码专家 Ron Rivest 设计的 RC4 加密算法，提供无加密、40 位密钥和 104 位密钥 3 种不同实现方式。

无加密表示数据以明文方式传输，能够接入 WLAN 的任何无线网络嗅探器都可以侦听发送的数据，因此无加密不提供任何保密性。40 位和 104 位密钥长度可向用户提供两种不同加密强度选择，但有些无线网络适配器只支持其中一种密钥；如果无线网络适配器同时支持两种密钥，自然应当使用 104 位密钥。只有当无线客户端的密钥和服务设置标识（Service Set Identity，SSID）与接入点完全相同时，客户端才能接入 WLAN。

SSID 用于标识特定 WLAN 的名称，用户在配置 WLAN 时，可以选择任意 SSID 名称，但不能与扫描范围内的其他 WLAN 同名。由于 WEP 使用共享密钥加密和解密数据，在有固定基础设施条件下，必须在无线 AP 和所有无线客户端上配置密钥。在无固定基础设施条件下，需要在所有无线客户端上配置密钥。

10.2.2 WEP 加密与解密

WEP 加密过程如图 10-7 所示。40 位或 104 位初始密钥与 24 位初始向量（Initialization Vector，IV）连接起来，生成 64 位或 128 位中间密钥；中间密钥通过 RC4 加密算法生成一串与明文流按位异或的密钥流，密钥流的长度与明文流相同。RC4 加密算法的核心是伪随机数生成器（Pseudo Random Number Generator，PRNG），其算法效率大约是 DES 的 10 倍。WEP 设置初始向量的目的是尽可能避免因重复使用共享密钥而降低加密强度，由于每帧数据都使用新的初始向量，为破译共享密钥增加了难度。

明文与完整性校验值（Integrity Check Value，ICV）连接起来形成明文流，ICV 由 32 位循环冗余完整性校验算法 CRC32 通过计算明文生成，明文中添加 4 字节的 ICV 能够防止在数据流中插入文本试图破解密文消息。明文流与密钥流按位异或形成密文，密文再与

初始向量连接生成最终的密文消息。由于在明文中连接了 4 字节的 ICV 值，所以明文流比明文长 4 个字节。明文流与密钥流长度相同，因此密文与明文流具有相同长度。初始向量为 3 个字节，完整性校验值为 4 个字节，最终密文消息比明文多 7 个字节。

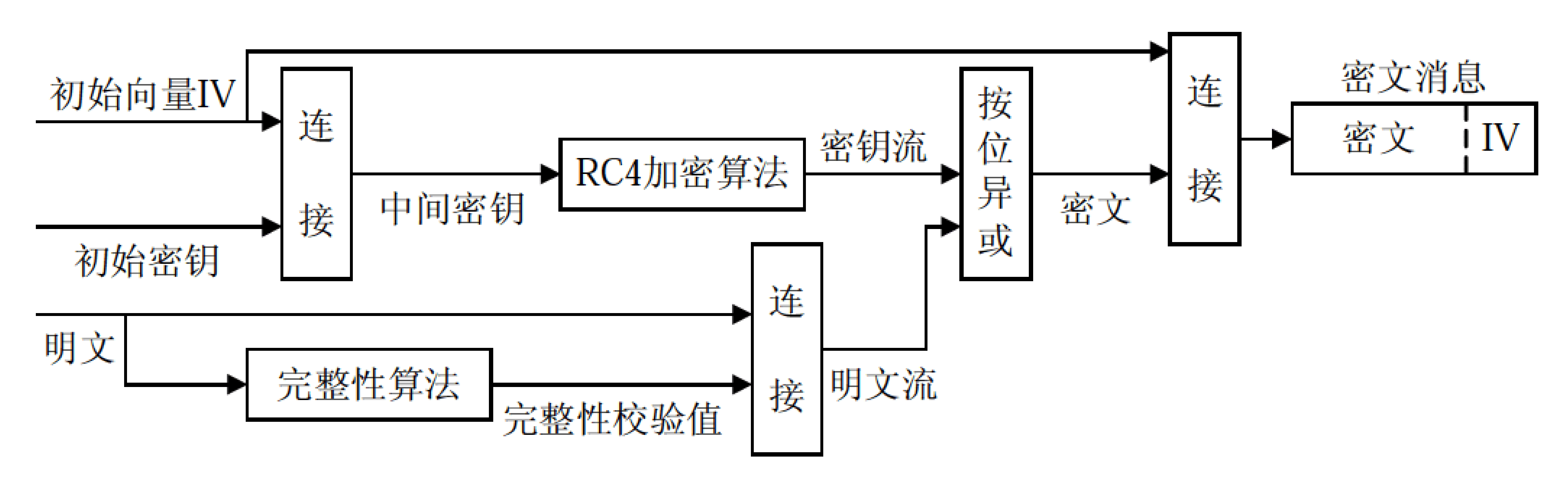


图 10-7 WEP 加密过程

WEP 解密是加密的逆过程，其解密过程如图 10-8 所示。初始密钥与密文消息中的初始向量连接后，生成 64 位或 128 位中间密钥。RC4 加密算法将中间密钥转换成密钥流，密钥流与密文消息中的密文异或后生成明文流，再将明文流拆分为明文和完整性校验值。同时计算明文的完整性校验值，并与明文流携带的完整性校验值比较。如两个校验值不同，表明该帧数据的完整性已经遭到破坏，则丢弃该帧。

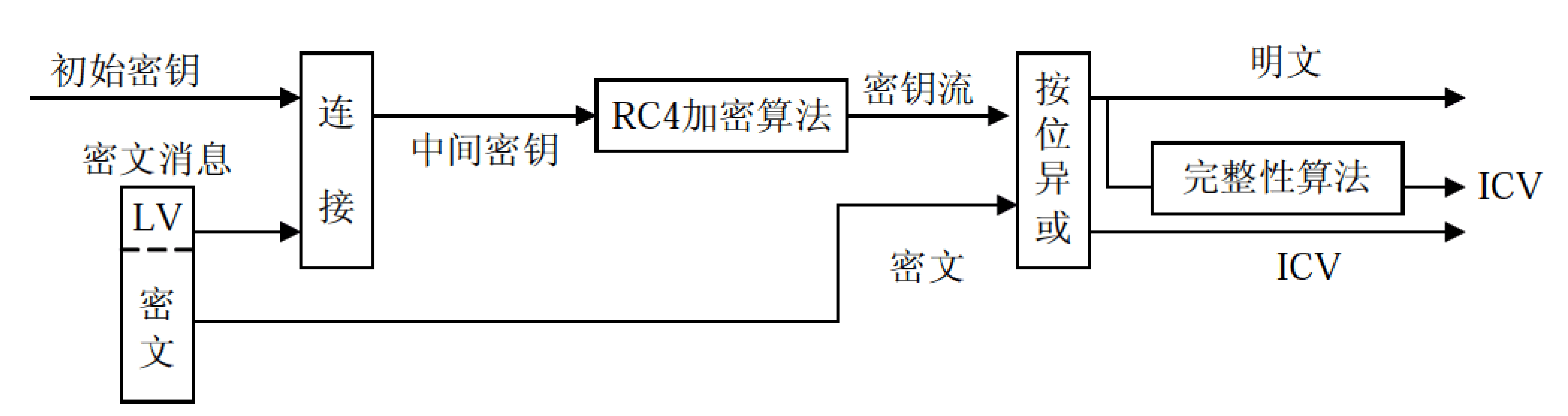


图 10-8 WEP 解密过程

10.2.3 IEEE 802.11 身份认证

IEEE 802.11 WLAN 具有开放系统认证（Open System Authentication）、封闭系统认证（Closed System Authentication）和共享密钥认证（Shared Key Authentication）3 种身份认证方式。开放系统认证是 IEEE 802.11 身份认证的默认方式。在开放系统认证方式下，无线 AP 并不要求无线客户端提供正确的 SSID。当无线客户端提交任意 SSID 认证请求时，无线 AP 通过广播自己的 SSID 来响应开放系统认证请求。因此，开放系统认证容许任意无线客户端接入无线 AP，即使输入错误的密钥，也可以同无线 AP 和其他客户端通信，只不过所有数据都采用明文方式传输。只有提供合法的共享密钥时，数据才以密文方式传输。开放系统认证强调的是简单易用，只能用于没有任何安全要求的场合。如果输入正确的密钥，开放系统认证能够提供数据保密性，但不具备身份识别功能。开放系统认证过程如图 10-9 所示。

封闭系统认证的安全级别略高于开放系统认证。在这种方式下，无线 AP 要求无线客户端必须提交正确的 SSID。只有认证双方具有相同的 SSID 时，才容许无线客户端接入 WLAN；否则，拒绝无线客户端的认证请求。封闭系统认证过程如图 10-10 所示。

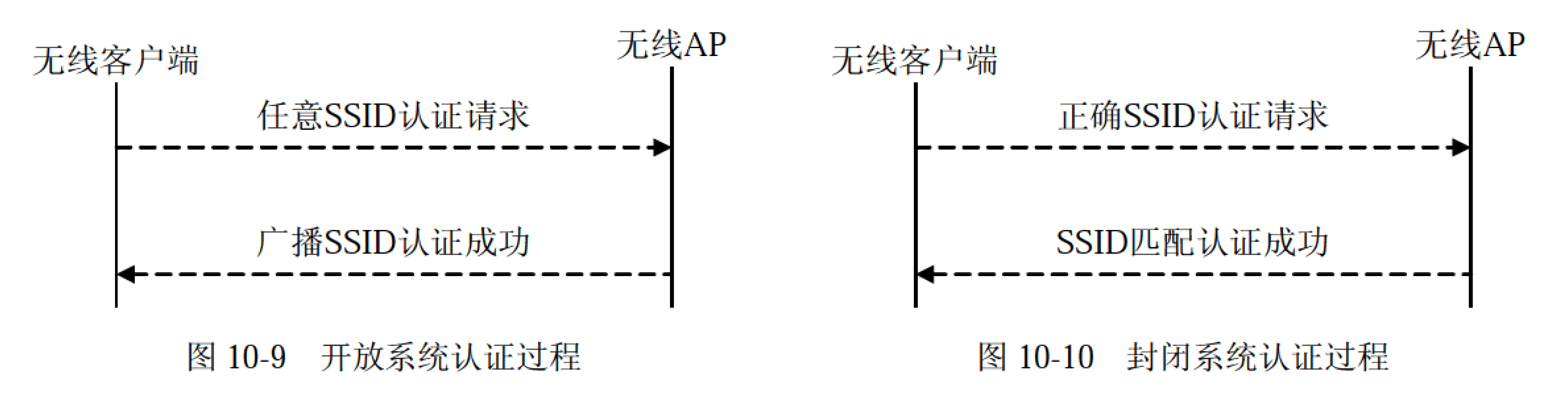


图 10-9 开放系统认证过程　　图 10-10 封闭系统认证过程

共享密钥认证就是采用 WEP 共享密钥和 SSID 来识别无线客户端的身份，只有提交正确的密钥和 SSID，无线 AP 才容许无线客户端接入 WLAN。显然，共享密钥认证的安全级别高于开放系统认证和封闭系统认证。WEP 共享密钥认证过程大致可以分为 4 步，如图 10-11 所示。首先，无线客户端向无线 AP 发送包含 SSID 的认证请求，无线 AP 接收到认证请求后，生成一个随机认证消息，作为认证请求的响应发送给无线客户端。随后，无线客户端用共享密钥加密随机认证响应并发送到无线 AP，无线 AP 采用共享密钥解密。如解密后的随机认证消息与发送的随机认证消息完全相同，则容许无线客户端接入；否则，判别无线客户端为非法用户，拒绝接入 WLAN。

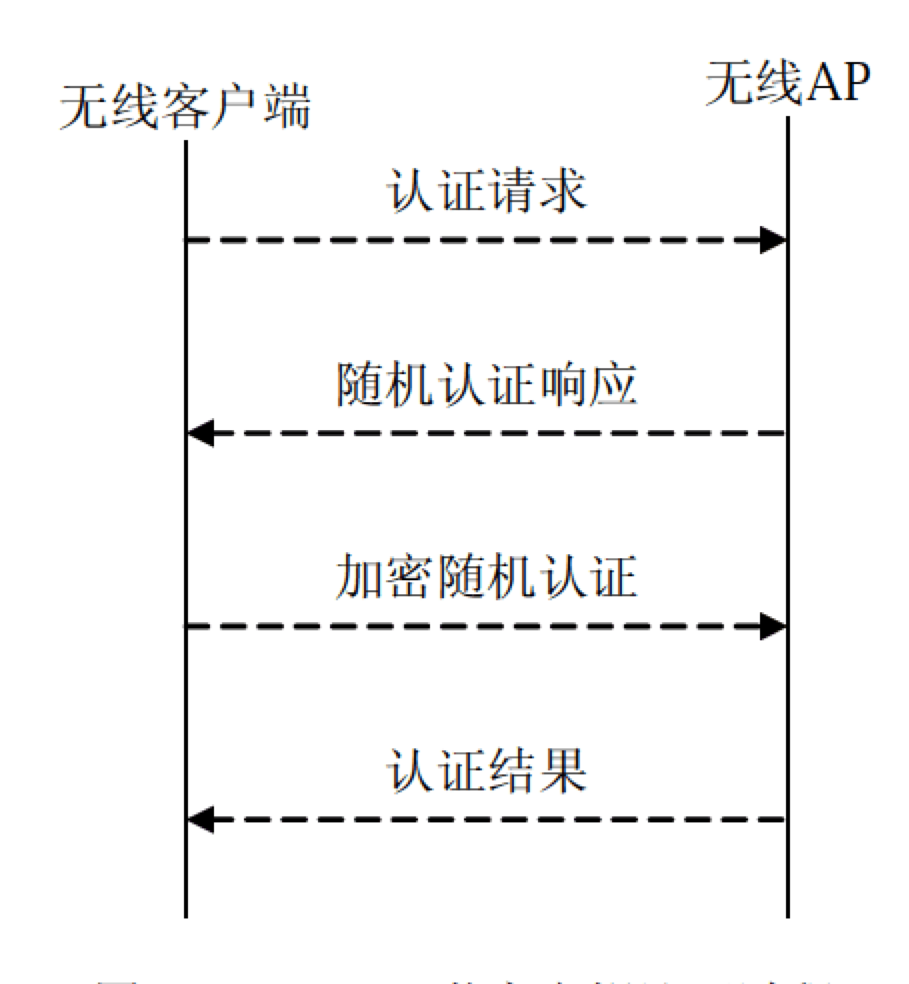


图 10-11 WEP 共享密钥认证过程

10.3 无线局域网有线等价保密安全漏洞

由于 WEP 在考虑安全性和易用性之间的均衡时，更多地倾向于易用性和加密算法的高效性，从而导致在 WEP 默认配置、加密、密钥管理和服务设置标识等方面存在大量的漏洞，进而为蓄意破坏 IEEE 802.11 系列 WLAN 上信息资源的保密性、完整性和有效性提供了条件。

10.3.1 WEP 默认配置漏洞

多数用户在安装无线网络适配器和无线 AP 设备时，只要求这些设备能够正常工作就可以了，很少考虑启用并正确配置无线安全性，通常都使用默认配置，而且正常工作后很

少再重新配置。开放系统认证是 WEP 的默认配置，它就好像在无线链路上设置了一个公共用户端口，任何无线客户端都可以接入并使用 WLAN 资源。例如，可以发送数据、监听通信内容、访问 WLAN 共享资源或通过无线 AP 访问有线网络上的共享资源，也可以窃取或破坏保密数据、安装病毒或“特洛伊木马”程序，甚至可以利用 Internet 连接发送病毒邮件或作为傀儡机向其他远程计算机发动攻击等。

10.3.2 WEP 加密漏洞

由图 10-7 所示的 WEP 加密过程可知，密文是通过明文流与密钥流按位异或形成的，然后密文再与初始向量连接构成密文消息。如果所有 WEP 帧都采用相同的密钥和初始向量加密，即使不知道共享密钥，利用重复使用的初始向量完全有可能破译出加密的 WEP 帧。破译的最简单方法就是对密文消息进行按位异或运算，然后剔除密钥流和初始向量，其结果是两个明文流的异或形式。如知道其中一个明文流，计算另一个明文流并不困难。

由于 IEEE 802.11 没有明确规定初始向量的使用方法，许多厂商在设计 WLAN 设备时，简单地将设备启动时的初始向量设置为 0，然后再逐次加 1。多数用户都会在每天早晨几乎相同的时间重新启动设备，大大增加了初始向量的重用率。只要获得足够多的相同初始向量，就有可能从密文消息中破译出密钥或明文。此外，初始向量只有 24 位，可用空间十分有限。就目前的计算能力而言，短时间内就可以穷举完所有的初始向量。有限的初始向量空间，也会导致密钥重用率提高，降低了密钥破译的难度。WEP 采用共享密钥加密和解密数据，如果需要更改密钥，就必须告知与之通信的所有节点，了解秘密的人越多，秘密信息也就变成了公开信息。

10.3.3 WEP 密钥管理漏洞

事实上，WEP 并没有提供真正意义上的密钥管理机制，需要依赖 Internet 工程任务组（Internet Engineering Task Force，IETF）提出的远程认证拨号用户服务（Remote Authentication Dial-In User Service，RADIUS）和扩展认证协议（Extensible Authentication Protocol，EAP）等外部认证服务，但多数小型企业或办公室在部署 WLAN 时，并不会使用造价昂贵的专用认证服务器。尽管 WEP 容许用户自己配置共享密钥，但手工配置共享密钥十分麻烦，且多数用户不熟悉密钥配置过程。无线网络适配器和无线 AP 在出厂时都带有 4 个默认的密钥，大多数用户一般都是从 4 个默认密钥中选择一个作为共享密钥。但厂商通常对密钥都进行了标准化，因此只要知道设备生产厂商和类型，通过检索厂商默认列表就有可能获得共享密钥。

WEP 也容许在无线客户端建立一个密钥映射表，记录 MAC 地址与共享密钥之间的对应关系；多个无线客户端之间直接利用 MAC 地址进行通信，MAC 地址的随机性很强。用 MAC 地址代替共享密钥从表面上看是提高了安全性，但众所周知，MAC 地址同样也是经过标准化的，如果能够知晓设备生产厂商，从 IEEE 标准网站 http://standards.ieee.org/regauth/

Oui/index.shtml 可以很容易检索到分配给厂商的 MAC 地址范围。

10.3.4 服务设置标识漏洞

服务设置标识 SSID 是 WLAN 的名称，也可以将一个 WLAN 分为多个要求不同身份认证的子网，用于区分不同的服务区。IEEE 802.11 采用 SSID 实现基本的资源访问控制，防止未经授权的无线客户端进入 WLAN 子网。无论是有固定基础设施还是无固定基础设施的 WLAN，无线客户端都必须出示正确的 SSID 才能访问无线 AP 或其他无线客户端。事实上，SSID 只是一个简单的口令身份认证机制。

多数制造商在其生产的无线 AP 中设置了默认 SSID，甚至在设备使用说明中明确指出默认的 SSID。如果部署 WLAN 时不改变厂商默认的 SSID，任何人通过网上检索或安装指南都能轻易地获得默认 SSID。只要将无线客户端的 SSID 修改成无线 AP 默认的 SSID，就有可能非法接入 WLAN。

此外，同一个生产厂商的无线 AP 和无线网络适配器一般具有相同的默认 SSID。即使不知道默认的 SSID，只要使用同一厂商的无线网络适配器也可以非法接入无线 AP。还有一些厂商使用无线网络适配器的半个 MAC 地址作为默认 SSID，MAC 地址采用十六进制数字表示，长度为 6 个字节。前 3 个字节是 IEEE 分配给厂商的唯一标识 OUI（Organizationally Unique Identifier），后 3 个字节为网络适配器的唯一标识编码。由于同一个厂商的 OUI 是完全相同的，因此无论使用前半个还是后半个 MAC 地址作为默认 SSID，检索或推测出默认 SSID 并不是一件十分困难的事情。此外，著名的 2600 黑客杂志网站收集了几乎所有厂商的默认 SSID 和 WEP 密钥（http：//mediawhore.wi2600.org/nf0/wireless/ssid_defaults/）。目前市场上无线 AP 主要生产厂商使用的默认 SSID 和 IEEE 分配的 MAC 地址 OUI 如表 10-1 所示。

表 10-1 无线 AP 主要生产厂商默认 SSID 和 OUI

厂 商 名 称	默认 SSID	OUI
Cisco	tsunami	00-40-96
Linksys	linksys	00-04-5A
TP-LINK	wireless	00-0A-EB
ACCTON	WLAN	00-00-E8
Compaq	compaq	00-02-A5
Intel	intel，xlan，101	00-02-B3
AboveCable	CTC	00-0D-08
3COM	101	00-00-86
Dell	wireless	00-06-5B
SMC Networks	WLAN	00-04-E2

10.4　无线局域网安全威胁

10.4.1　无线局域网探测

1．战争驱车探测

无线网络攻击步骤与有线网络攻击类似，第一步都是要发现目标无线网络。多数机构都使用防火墙作为内部网络的第一道安全防线，因为防火墙能够有效地隔离内部网和开放的 Internet。但内部网中私自与 Internet 连接的调制解调器给内部网安全留下了隐患，如使用“战争拨号器”（War Dialers）软件随机拨打电话号码，能够迅速发现接入 Internet 的调制解调器。人们将寻找隐藏调制解调器的方法称为“战争拨号”（War Dialing）技术，其中“战争拨号”中的“战争”（War）一词取自著名电影《真假战争》（War Games）。

由于探测 WLAN 的方法有些类似“战争拨号”技术，人们便将携带移动设备驱车到处转悠寻找 WLAN 的方法称为“战争驱车”（War Driving）技术。“战争驱车”、“战争驾驶”或“战争驾车”都是 War Driving 的直译；事实上，War Driving 是泛指各种搜索无线局域网信息的技术，也许用无线局域网探测或扫描能更好地表示 War Driving 的含义。目前网络上有 Windows、UNIX、Linux 和 Mac OS 操作系统平台下运行的多种无线局域网探测和定位软件，表 10-2 列举了部分常用开放源码或非商业无线局域网探测软件，同时还给出了这些软件的名称、当前最高版本、操作系统平台和下载地址，其中最著名的 WLAN 探测和定位软件是由 Marius Milner 开发的 NetStumbler。

表 10-2　常用开放源码或非商业 WLAN 探测软件

程序名称	最高版本	操作系统	软件类型	下载地址
NetStumbler	0.4.0	Windows	免费	http://www.netstumbler.com/downloads/
MiniStumbler	0.4.0	Windows CE	免费	http://www.netstumbler.com/downloads/
Kismet	04-10-R1	UNIX、Linux	开放源码	http://www.kismetwireless.net/
SSIDSniff	0.4.0	UNIX、Linux	开放源码	http://www.netsecurity.about.com/gi/dynamic/
WiFi Scanner	0.9.6	UNIX、Linux	开放源码	http://sourceforge.net/projects/
IStumbler	92	Mac OS X	开放源码	http://www.istumbler.net/
Wifimap	0.3.1	UNIX、Linux、Windows	开放源码	http://sourceforge.net/projects/wifimap/
Wellenreiter	1.9	UNIX、Linux	开放源码	http://www.remote-exploit.org/
KisMAC	0.009a	Mac OS X	开放源码	http://kismac.binaervarianz.de/
Prismstumbler	0.7.3	UNIX、Linux	开放源码	http://prismstumbler.sourceforge.net/

2．NetStumbler 简介

NetStumbler 0.4.0 要求在 Windows 2000、Windows XP 或更高操作系统版本下运行；虽然未公开源代码，但可以免费使用；目前支持 IEEE 802.11a、802.11b 和 802.11g 无线网络

适配器和全球定位系统 GPS。事实上，NetStumbler 并不是一个专用的 WLAN 探测和定位工具。其主要功能是 WLAN 安全审计、信号质量检测、安装位置选择、探测与定位，安全审计供网络管理员检测自己周围是否存在恶意 WLAN，信号质量检测可以确定覆盖区内的信号质量及覆盖范围，安装位置选择能够为 WLAN 选择干扰最小的安装位置，探测和定位结合 GPS 实现“战争驱车”功能。

NetStumbler 通过向周围的 WLAN 发送探测请求，能够获得目标 WLAN 的 MAC 地址、SSID、无线 AP 名称、数据传输速率、设备制造商、AP 网还是自组网、是否加密、IP 地址、信号强度及所在经纬度等信息。

10.4.2 无线局域网监听

无线局域网监听的机制和方法与广播机制以太局域网相同，需要利用无线网络适配器的混杂工作模式从数据链路层实时截获数据帧，然后通过网络协议解析所获取数据帧的内容。目前绝大多数无线 AP 属于无线集线器，对于无线集线器共享网络环境，只要将网络适配器设置成混杂工作模式，就可以监听到整个 WLAN 内的数据帧流量；而无线交换 AP 交换网络环境给 WLAN 监听增加了困难，由于每个无线客户端都是一个独立的网段，不同网段之间通过交换 AP 内部的网桥互联，因此网络适配器混杂工作模式并不能截获到其他网段的任何数据帧。如果利用无线集线器将无线交换网络转换成共享网络，就有可能实现对无线交换网络的监听。

目前有许多软件工具支持无线局域网监听，除 6.2 节介绍的 Tcpdum、Ethereal、Ngrep 等网络数据包采集与分析工具之外，诸如 Airopeek、Kismet、Airsniffer、AirTraf、Airjack、LibRadiate、Mognet、APsniff 等都可以实现无线局域网监听。如果 WLAN 以明文方式传输数据，这些无线局域网监听工具都可以解析出传输内容。即使 WLAN 采用了加密保护机制，仍无济于事，非法用户甚至不需要自己从密文消息中破译密钥，因为有众多免费 WLAN 密钥破译软件可供使用。例如，Wepcrack、Airsnort、Weplab、Aircrack、Airsnarf、Asleap、WepAttack 都是当前网络上流行的 IEEE 802.11 WEP 密钥破译软件。多数破译软件只要采集 500 万～1000 万左右的加密分组，利用 WEP 加密漏洞就可以计算出 WEP 密钥；另一些破译软件则采用传统的字典攻击手段，试图猜测出密钥。

10.4.3 无线局域网欺诈

无线局域网欺诈（Fraud）就是利用默认配置漏洞、加密漏洞、密钥管理漏洞和服务设置标识漏洞等突破身份认证的封锁，假冒合法无线客户端或无线 AP 骗取 WLAN 的信任，窃听重要机密信息或非法访问网络资源的攻击行为。尽管 IEEE 802.11 WLAN 开放系统认证容许所有无线客户端接入无线 AP，但没有正确的共享密钥，欺诈客户端只能与无线 AP 或其他无线客户端明文通信，并不能窃听到以密文传输的重要机密信息；封闭系统认证则要求无线客户端提供正确的 SSID；而共享密钥认证不仅要求无线客户端提供正确的共享密

钥，还要求出示正确的 SSID，只有通过身份认证的无线客户端才能接入 WLAN。由此可以看出，实现欺诈的关键是突破身份认证，而通过身份认证最简便的办法就是设法获得 SSID 和 WEP 共享密钥。如前 SSID 漏洞所述，获取 SSID 并不困难，窃取或破译共享密钥才是 WLAN 欺诈的关键要素。

除了使用众多免费的 WEP 共享密钥破译软件之外，由于 WEP 共享密钥认证过程相对简单，通过伪造合法的共享密钥认证过程，仍然有可能实现欺诈意图。在共享密钥认证方式下，无线 AP 收到认证请求后，以明文形式发送一个 128 位的随机认证消息，随机认证消息由共享密钥和初始向量通过 RC4 加密算法生成，无线客户端用共享密钥对随机认证消息加密后回送给无线 AP。如果能够积累大量回送给无线 AP 的加密随机认证报文，就有可能破译出无线客户端对明文流加密使用的密钥流，因为加密随机认证报文中隐藏了密钥流。一旦窃听到发送给客户端的明文随机认证响应，就可以用密钥流伪造一个合法的加密随机认证报文，无线 AP 必然错误地认为这是一个合法的无线客户端。共享密钥认证欺诈过程如图 10-12 所示。

IEEE 802.11 WLAN 除采用 SSID 和 WEP 共享密钥安全机制之外，MAC 地址过滤也是重要的安全措施之一。将 SSID、MAC 地址过滤和 WEP 共享密钥多种安全机制组合起来，能够在很大程度上降低安全威胁，多数无线 AP 在开放系统认证、封闭系统认证和共享密钥认证方式下都支持 MAC 地址过滤。MAC 地址过滤就是用无线网络适配器的物理地址来确定无线客户端的合法性。在 MAC 地址过滤之前，需要在无线 AP 建立容许访问 WLAN 的 MAC 地址列表；只有当无线客户端提交的 MAC 地址能够与无线 AP 建立的 MAC 地址列表匹配时，才容许访问 WLAN。

如果在封闭系统认证方式下配置了 MAC 地址过滤，无线客户端不仅要向无线 AP 出示正确的 SSID，还需要提交合法的 MAC 地址。无线客户端首先向无线 AP 发送 SSID 认证请求，如果是开放系统认证，则可以发送任意 SSID 认证请求。如果提交的 SSID 能够与无线 AP 的 SSID 匹配，无线 AP 将返回认证成功应答。但此时无线客户端还不能接入 WLAN，还需继续向无线 AP 发送 MAC 地址连接请求，如提交的 MAC 地址位于合法 MAC 地址列表，则无线 AP 授权无线客户端的连接请求。

尽管 MAC 地址过滤机制增强了 WLAN 的安全性，但也为无线局域网欺诈提供了机会。由于无线客户端以明文方式向无线 AP 发送 MAC 地址连接请求，利用无线局域网监听工具很容易窃取 WLAN 中其他无线客户端向无线 AP 发送的合法 MAC 地址。此外，如果能知道无线客户端使用的无线网络适配器生产厂商，破译 MAC 地址要比破译 WEP 共享密钥容易得多，因为 MAC 地址是通过标准化生成的。通过伪造合法 MAC 地址即可实现无线局域网欺诈。操作系统和无线网络适配器支持 MAC 地址重新配置功能，也为 MAC 地址欺诈提供了方便。封闭系统认证 MAC 地址欺诈过程如图 10-13 所示。

如果伪造 MAC 地址的无线客户端和合法 MAC 地址的无线客户端同时在线，必然会破坏 ARP 缓存表，所以利用 MAC 地址欺诈接入 WLAN 之前，需要用 WLAN 监听工具确认合法 MAC 地址是否在线。

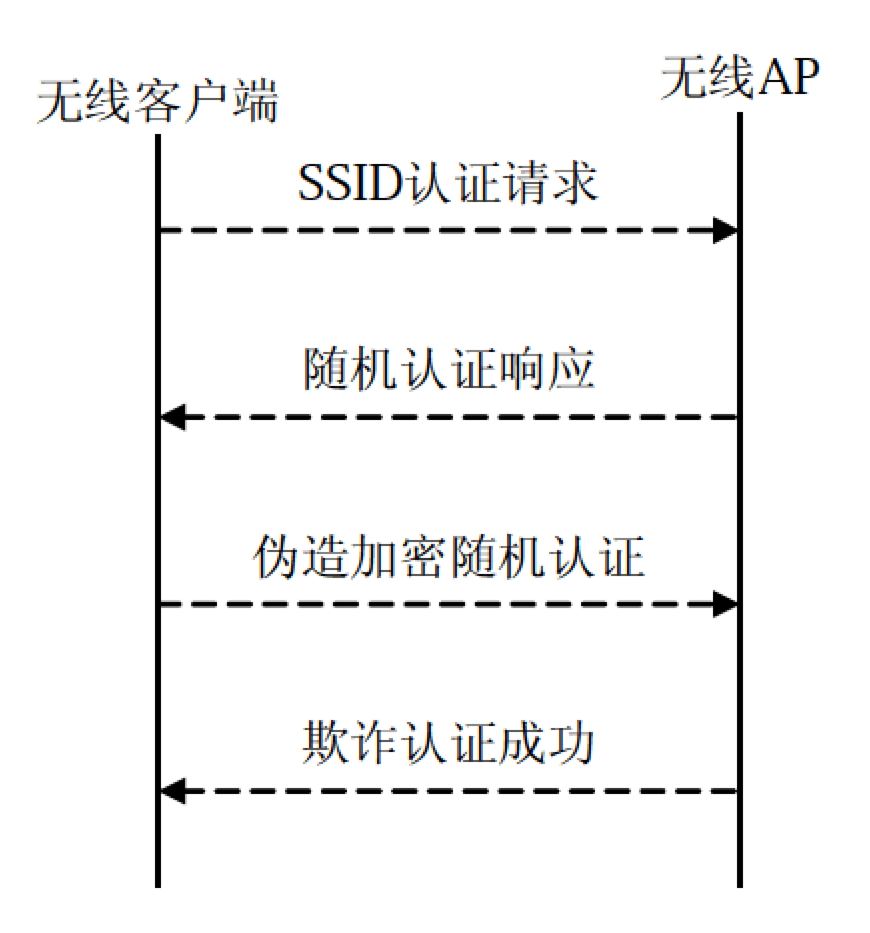



图 10-12 共享密钥认证欺诈过程

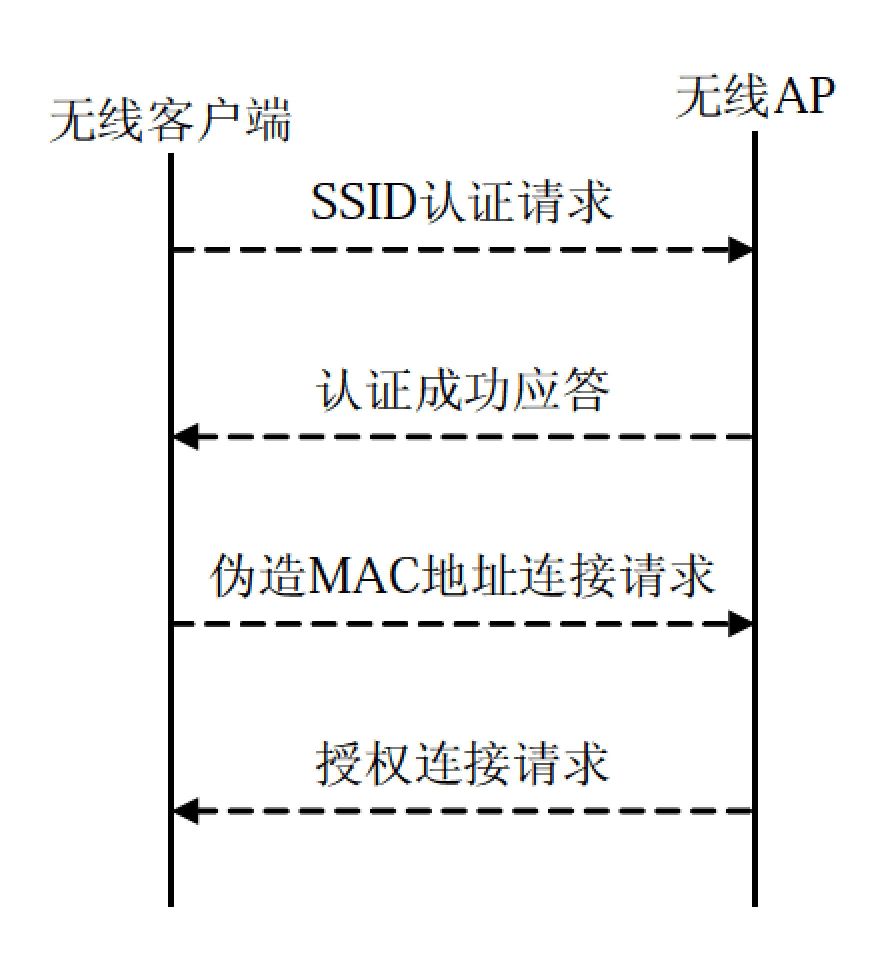


图 10-13 封闭系统认证 MAC 地址欺诈过程

10.4.4 无线 AP 欺诈

无线 AP 欺诈（Rogue）是指在 WLAN 覆盖范围内秘密安装无线 AP，窃取通信、WEP 共享密钥、SSID、MAC 地址、认证请求和随机认证响应等保密信息的恶意行为。事实上，WLAN 固有的性质不仅为无线局域网欺诈提供了方便，也为在 WLAN 附近安装欺诈无线 AP 提供了便利条件。

为了实现无线 AP 欺诈目的，首先需要利用 Netstumbler 等 WLAN 探测和定位软件获得合法无线 AP 的 SSID、信号强度、是否加密等信息。根据信号强度能够将欺诈无线 AP 秘密安装到合适位置，确保无线客户端可以在合法 AP 和欺诈 AP 之间切换。此外，自然还需要将欺诈 AP 的 SSID 设置成合法无线 AP 的 SSID 值。如果 WIAN 采用开放系统认证或封闭系统认证，无线 AP 欺诈此时便告成功。如果 WLAN 采用共享密钥认证，还需要设法获得 WEP 共享密钥才能欺诈成功。

发现欺诈无线 AP 的最简单方法就是使用无线局域网探测软件，因为无线局域网探测软件的基本功能就是试图发现非法无线 AP，但前提是欺诈无线 AP 采用了开放系统认证，因为在封闭系统认证或共享密钥认证方式下，无线 AP 并不广播自己的 SSID。WLAN 欺诈无线 AP 如图 10-14 所示。

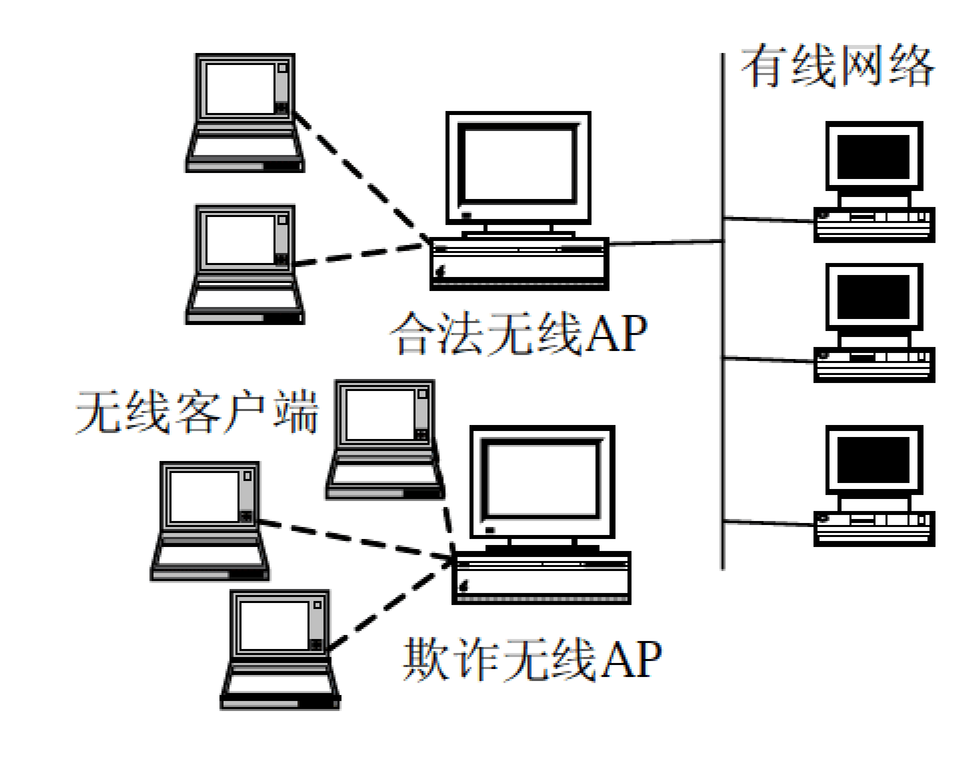


图 10-14 WLAN 欺诈无线 AP

10.4.5 无线局域网劫持

无线局域网劫持（Hijack）是指通过伪造 ARP 缓存表使会话流向指定恶意无线客户端的攻击行为。无线局域网劫持原理与有线网络的会话劫持相同，主要是利用了 ARP 协议中

存在的请求与应答报文漏洞。通过网络层将 MAC 地址隐藏起来，使用统一的 IP 地址通信可以使 TCP/IP 协议与具体的物理网络无关，但主机在数据链路层必须使用 MAC 地址才能实现通信，正是 ARP 协议提供了 IP 地址到 MAC 地址的映射服务。

ARP 协议采用动态绑定（Dynamic Binding）方式解析目的主机的 MAC 地址，当主机发送数据时，首先查询本机的 ARP 缓存表，如检索到目的 IP 地址对应的 MAC 地址，将 MAC 地址封装在数据帧头内就可以实现数据链路层之间的通信。如果未检索到目的 IP 地址对应的 MAC 地址，则在本网段内广播 ARP 请求报文，只有同目的 IP 地址相同的主机才回送包含 MAC 地址的 ARP 应答报文。如果目的 IP 地址位于其他网络，主机将 ARP 请求报文发送给路由器，路由器再报告自己的 MAC 地址，然后由路由器转发数据报文。

由于在设计 ARP 协议时没有考虑 ARP 发送请求进程与侦听应答进程之间的关联，换句话说，发送主机接收到 ARP 应答报文时，并不清楚是否曾发送过 ARP 请求报文，主机只要接收到 ARP 应答报文，就将 MAC 地址保存到 ARP 缓存表中。正是 ARP 发送请求进程与侦听应答进程之间的无关联性，为通过伪造 MAC 地址实现会话劫持提供了机会。

同一网段及不同网段内的无线局域网劫持过程如图 10-15 所示。假设恶意无线客户端的 IP 地址和 MAC 地址分别为 192.168.0.1、00-00-86-01-02-0B；路由器的 IP 地址和 MAC 地址分别为 192.168.0.3、00-00-86-01-02-0D。如果恶意无线客户端希望劫持同一网段内 IP 地址为 192.168.0.0 的无线客户端会话，只要他知道对方的 IP 地址，并向其发送一个包含自己 00-00-86-01-02-0B MAC 地址的 ARP 应答报文，无线客户端便会错误地认为 00-00-86-01-02-0B 就是目标主机的 MAC 地址，此时无线客户端的所有报文就将被劫持到恶意无线客户端。如果恶意无线客户端希望劫持位于另一网段内 IP 地址为 192.168.0.2 的无线客户端会话，则必须向路由器发送伪造 MAC 地址 00-00-86-01-02-0B，使路由器 ARP 缓存表错误地将无线客户端的 IP 地址 192.168.0.2 映射成 00-00-86-01-02-0B 恶意 MAC 地址，路由器便会将无线客户端发送的所有报文错误地转发到恶意无线客户端。

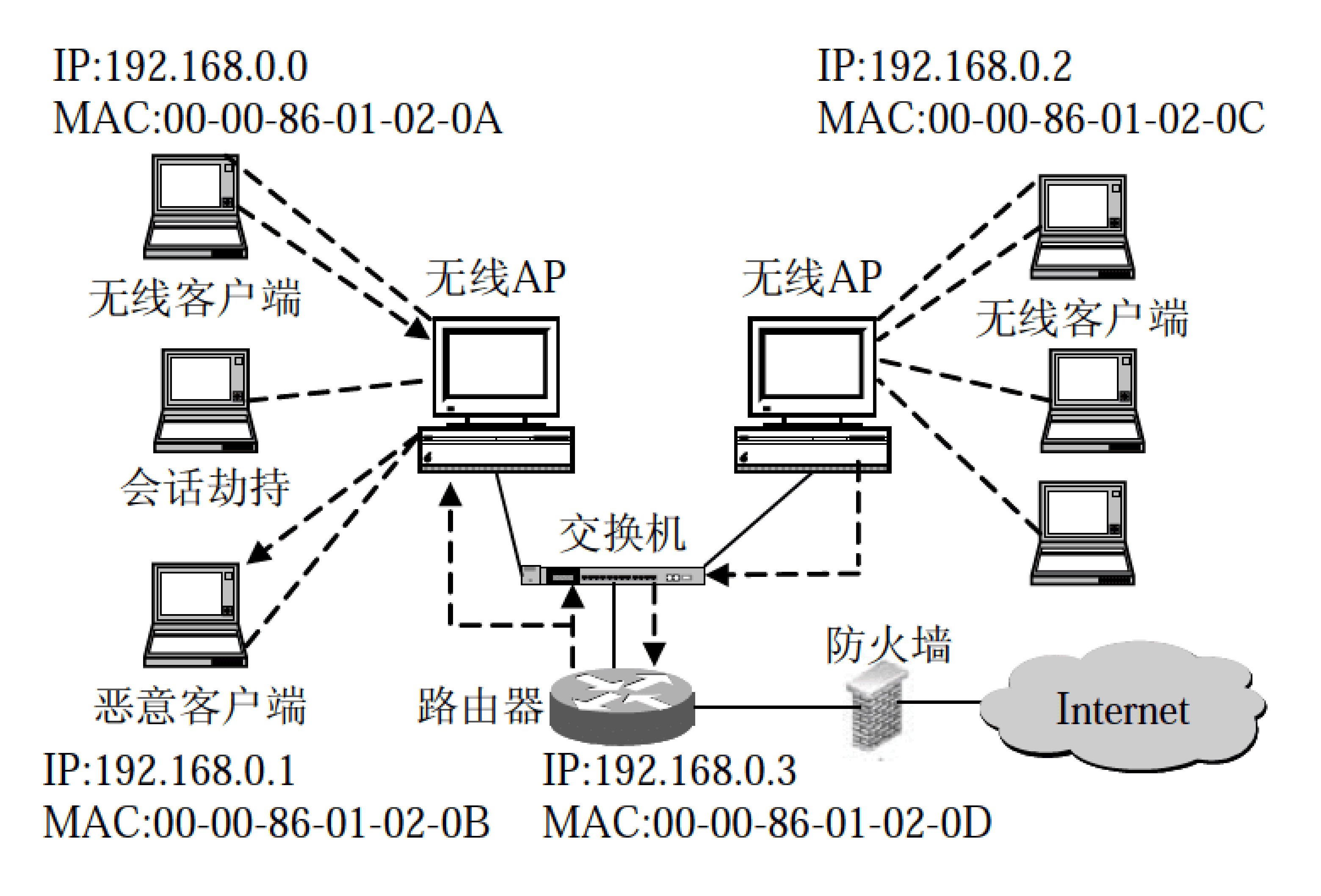


图 10-15 同网段及不同网段 WLAN 劫持过程

目前网络上存在大量免费的会话劫持软件，甚至有些劫持软件还提供源代码，只要在

搜索引擎中输入关键词 ARP Spoof 就可以发现众多的劫持软件。例如，Dsniffer、Bktspibdc、WCI、ARPOC2、Hunt、Fake、ARPtool 等都是典型的 ARP 会话劫持软件。从无线局域网会话劫持的原理可以看出，能够实现会话劫持的前提是 ARP 协议使用了动态绑定机制。因此，只要采用静态 ARP 缓存表就可以有效地防止这种会话劫持攻击，但手工维护大量的静态 MAC 地址会给安全管理增加额外的维护负担。

10.5 无线保护接入安全机制

为了解决 IEEE 802.11 系列无线局域网 WEP 安全机制存在的各种安全漏洞与威胁，Wi-Fi 联盟于 2003 年 2 月正式推出了无线局域网无线保护接入（Wi-Fi Protected Access，WPA）安全机制。WPA 采用临时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）加强了数据传输的保密性；采用基于端口的网络接入控制协议（Port-based Network Access Control Protocol）IEEE 802.1X 和扩展认证协议 EAP 相结合的方法提高了身份认证的可信度和密钥管理的安全性。WPA 不仅适应企业网络环境，也可以用于小型、家庭办公网络环境（Small Office/Home Office，SOHO），并且能够兼容 WEP 和 IEEE 标准委员会于 2004 年 6 月宣布的 IEEE 802.11i 新一代无线局域网安全标准。如果无线 AP 和无线网络适配器支持 WPA，只要在无线 AP 安装 IEEE 802.1X 和 TKIP 协议软件，在无线客户端安装 IEEE 802.1X、TKIP 和 EAP 协议，即可将企业无线局域网从脆弱的 WEP 轻松升级到具有互操作性和健壮、安全的 WPA。

10.5.1 WPA 过渡标准

事实上，WPA 是 IEEE 802.11i 新一代无线局域网安全标准的子集。Wi-Fi 联盟考虑到 IEEE 802.11i 安全机制获得 IEEE 标准委员会批准还需要一段时间，等待新一代安全标准出台必然会阻止 WLAN 产品的研发和市场发展速度；由于已经发现 WEP 存在多种安全漏洞和威胁，生产厂商纷纷开发各自的 WLAN 安全解决方案，但不同厂商提出的安全解决方案缺少互操作性。正是在这种情形下，Wi-Fi 联盟在 IEEE 802.11i 出台之前推出了 WPA，作为 IEEE 802.11i 的过渡中间标准，确保 WLAN 在过渡期内的安全性。Wi-Fi 联盟是 IEEE 802.11i 标准的主要参与者之一，所以在规划 WPA 时就考虑了对市场上广泛使用的 WEP 和未来安全标准的兼容性。因此，不需要对现有 WLAN 结构进行过多的改变，WEP 的软件和固件就可以很容易地升级到 WPA，WPA 也可以方便地升级到 IEEE 802.11i 标准。

10.5.2 IEEE 802.11i 标准

IEEE 802.11i 标准的全称是“IEEE 信息技术标准系统之间的通信和信息交换局域网和城域网特殊需求——第 11 部分：无线局域网介质接入控制和物理层规范——修正 6：介质

接入控制安全增强（Medium Access Control Security Enhancements）”，Wi-Fi 联盟则将 IEEE 802.11i 标准称为第二代无线保护接入（Wi-Fi Protected Access 2，WPA2）。IEEE 802.11i 在修正 WEP 已知缺陷的基础上，基于 IEEE 802.1X 认证协议、预先认证（Pre-Authentication，PA）、密钥体系（Key Hierarchy，KH）、密钥管理（Key Management，KM）、密码和认证协商（Cipher and Authentication Negotiation，CAN）、临时密钥完整性协议 TKIP、计数模式/密码块链接消息认证码 CCMP 协议（Counter-mode/CBC-MAC Protocol，其中 CBC-MAC 是指 CipherBlock Chaining Message Authentication Code）和无线健壮认证协议（WirelessRobust Authenticated Protocol，WRAP）等安全机制，提出了健壮安全网络（Robust Securitv Network，RSN）的概念，从数据保密、密钥管理、身份认证、访问控制、消息完整性校验等多个方面加强了 WLAN 的安全性。

尽管 IEEE 802.11i 标准比 WPA 具有更高的安全级别，但由于实现成本较高，将主要用于政府、国防、公安、金融、企业等对信息安全有特殊要求的网络环境，而 WPA 更适用于 SOHO 网络环境，因此多数网络安全专家认为 IEEE 802.11i 标准并不能完全取代 WPA。WPA 与 IEEE 802.11i 标准之间的关系如图 10-16 所示，WPA 提供了 IEEE 802.11i 标准中的 IEEE 802.1X 认证协议、密钥体系、密钥管理、密码和认证协商及临时密钥完整性协议主要安全机制。

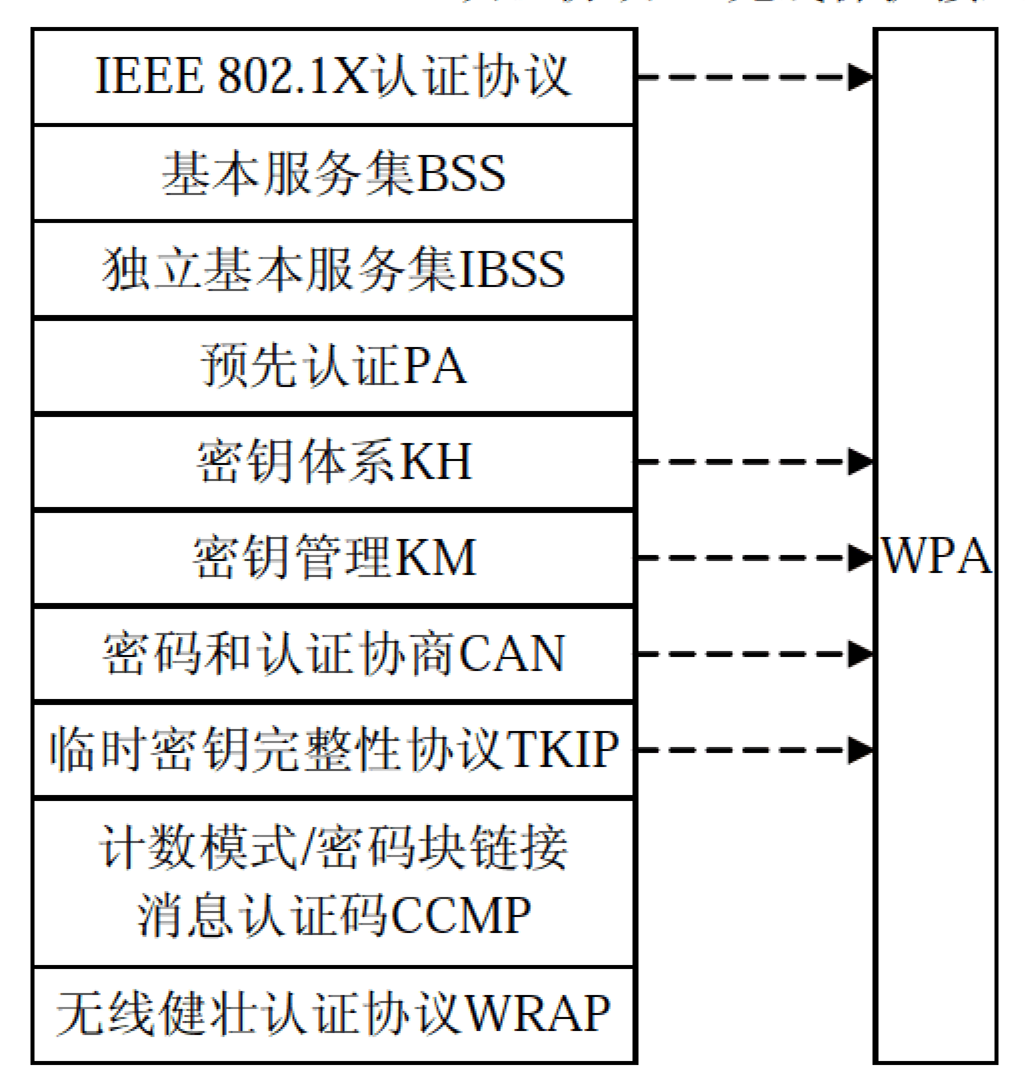


图 10-16　WPA 与 IEEE 802.11i 标准之间的关系

10.5.3　WPA 主要特点

相对于 WEP，WPA 提供了比较完善的数据加密和用户身份认证功能。WEP 使用安全性较差的 40 或 104 位密钥长度，24 位初始向量空间，用 WEP 密钥本身验证无线客户端身份。WPA 采用具有消息完整性校验（Message Integrity Check，MIC，也称为 Michael 码）

功能的 TKIP 加密技术代替了容易破译的 WEP 加密体制，并且将初始向量、密钥长度分别扩大到 48 和 128 位，提高了破译 TKIP 密钥的难度。同时使用 IEEE 802.1X 认证协议、扩展认证协议 EAP 或预先共享密钥（Pre-Shared Key，PSK）技术，提供了无线客户端和认证服务器之间的双向认证功能，解决了 WEP 单向认证的缺陷。此外，WPA 向下兼容 WEP，能够容易地通过软件或固件升级现有的 WEP 无线 AP 和无线网络适配器，而且不会影响无线网络的性能。WPA 不仅适用于 SOHO 网络环境，也适用于企业或小型商业环境，只有通过身份认证的合法用户才能访问 WLAN 资源。

10.5.4 IEEE 802.11i 主要特点

IEEE 802.11i 标准或 WPA2 不仅支持 IEEE 802.1X、EAP 或 PSK，而且定义了 CCMP 和 WRAP 高级加密标准（Advanced Encryption Standard，AES）。AES 是美国商业部和国家标准技术协会批准的美国官方加密标准，能够满足官方政府的安全需求。但 AES 不能通过软件或固件方式升级 WEP 或 WPA 设备，需要购置支持 AES 的无线 AP 和无线网络适配器。尽管 IEEE 802.11i 标准定义了 TKIP、CCMP 和 WRAP 3 种加密机制，但只有 CCMP 和 WRAP 才是实现 RSN 概念的强制要求，IEEE 802.11i 标准规定 WRAP 仅是一种可选加密机制。WEP、WPA 和 IEEE 802.11i 标准的主要不同点，如表 10-3 所示。

表 10-3 WEP、WAP 与 IEEE 802.11i 的主要不同点对比

主要安全机制	WEP	WAP	IEEE 802.11i
数据加密体制	RC4	TKIP	CCMP 或 WRAP
密钥长度	40 或 104 位	128 位	128 位
初始向量长度	24 位	48 位	48 位
完整性校验算法	CRC32	Michael（MIC）	CCM
完整性校验内容	仅数据部分，头部无校验	数据和头部都校验	数据和头部都校验
密钥管理协议	无	IEEE 802.1X 和 EAP	IEEE 802.1X 和 EAP
密钥管理方式	固定密钥、人工分发	动态事务密钥、自动分发	动态事务密钥、自动分发
身份认证协议	WEP 密钥	IEEE 802.1X 和 EAP	IEEE 802.1X 和 EAP

10.6 无线网络安全实用技术举例

10.6.1 802.11 规范的认证方式及其不足

WLAN 由于自身广播的特点，需要额外的机制去保证合法用户的接入和数据正常传输的完整及安全性。针对无线终端用户，IEEE 802.11 规范规定了两种机制：开放认证方式和共享密钥认证方式。还有其他两种机制，即使用 SSID 和基于 MAC 地址的认证也是被广泛采用的，同时使用 WEP 密匙也可被作为一种接入控制手段。

通过 SSID 可以实现 WLAN 的逻辑隔离。通常一个无线终端必须配置正确的 SSID 以便获许接入到 WLAN 的网络中来，但 SSID 没有提供任何的数据安全性功能，也没有真正地对无线终端进行认证。

开放认证方式允许任何的终端设备与 AP 进行认证并尝试发生通信。如果 AP 上没有采用加密方式，任何配置对应 SSID 的无线终端均可获许接入到网络中。当在 AP 上采用了 WEP 加密方式，WEP 密匙本质上成为一种接入控制方式。如果无线终端设备没有正确的 WEP 密钥，即使通过认证，无线终端也无法通过 AP 发送数据到其他的网络设备，或者将从 AP 发来的数据包解密。

共享密钥认证方式是 802.11 规范定义的第二种认证方式。共享密钥认证方式要求无线终端具备静态 WEP 密钥的配置。由于共享密钥认证方式存在严重的安全缺陷，不推荐使用。因为在共享密钥认证操作期间，AP 发送的认证响应的报文并没有对挑战正文进行加密，而无线终端直接将加密后的报文发回，所有的报文均可以被监听。入侵者可以利用这两个报文计算出 WEP 密钥，从而可正式连接到网络中。因为这个缺陷，共享密钥认证方式比开放认证方式更不安全。同样，共享密钥认证方式也不依赖于网络的 RADIUS 服务器。

MAC 地址认证方式并没有在 802.11 规范中定义。MAC 地址认证方式被用来增强 802.11 规范中定义的两种认证方式，更进一步地减少未经授权用户接入到网络的可能性。但由于 MAC 地址被作为明文发送，所以入侵者也很容易截获并假冒有效的无线终端。

10.6.2　建设安全的 802.11 网络——思科无线网络安全

认识到 802.11 网络认证和数据安全性的弱点后，为了给用户提供可扩展的、可管理的并且可靠的 WLAN 网络，思科采用标准的方法增强了 802.11 网络的认证和加密。实际上，无线网络的安全可以由 3 部分组成：认证的体系框架、认证算法和数据安全性加密算法。

思科无线网络安全套件由以下几部分组成：

（1）802.1X 认证体系

IEEE 802.1X 标准提供了可被多重认证方式使用的通用架构。

（2）LEAP 认证算法

支持集中式的、基于用户的并具备动态生成 WEP 密钥的认证方式。

（3）临时密钥完整性协议 TKIP

思科提供两种方式增强 WEP 的功能，即 MIC 和 PPK。

（4）采用报文完整性检测 MIC

有效地提供数据帧的真实性，以减少网络入侵者的攻击。

（5）每帧密钥（Per Packet Keying）

基于每个用户帧的加密，最大程度上减少入侵者生成 WEP 的攻击。

10.6.3　802.1X 认证架构

802.1X 认证架构已经被采用在 IEEE 802.11 工作组 I（TGI）中作为 802.11 MAC 层安

全的增强手段，如图 10-17 所示。

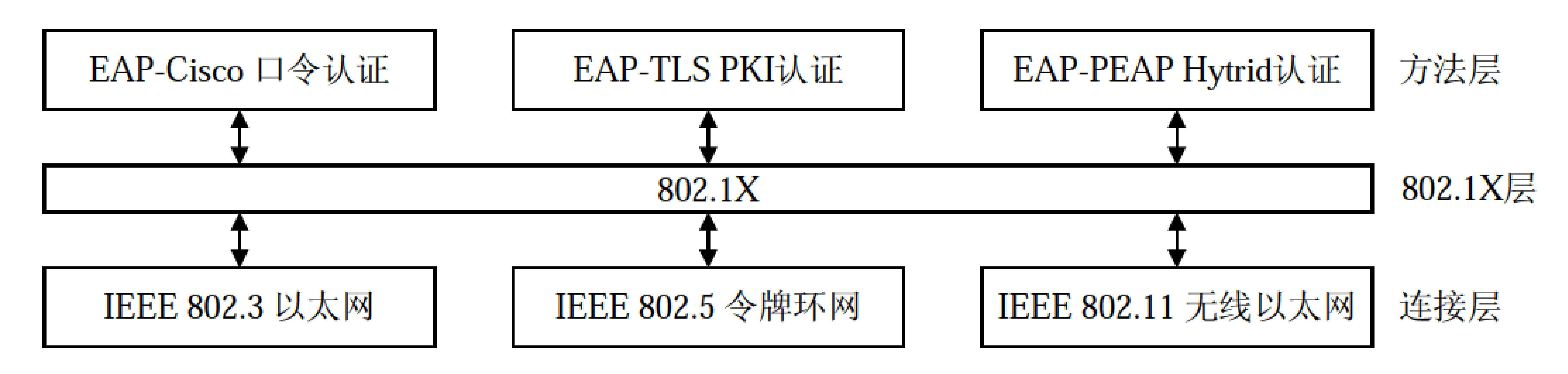


图 10-17　802.1X 网络层结构

完成 802.1X 认证需要 3 个实体。

（1）请求者：这个实体驻留在 WLAN 终端内。

（2）认证者：这个实体驻留在 AP 内。

（3）认证服务器：这个实体驻留在 RADIUS 服务器内。

图 10-18 给出了 802.1X 组件间操作流程。

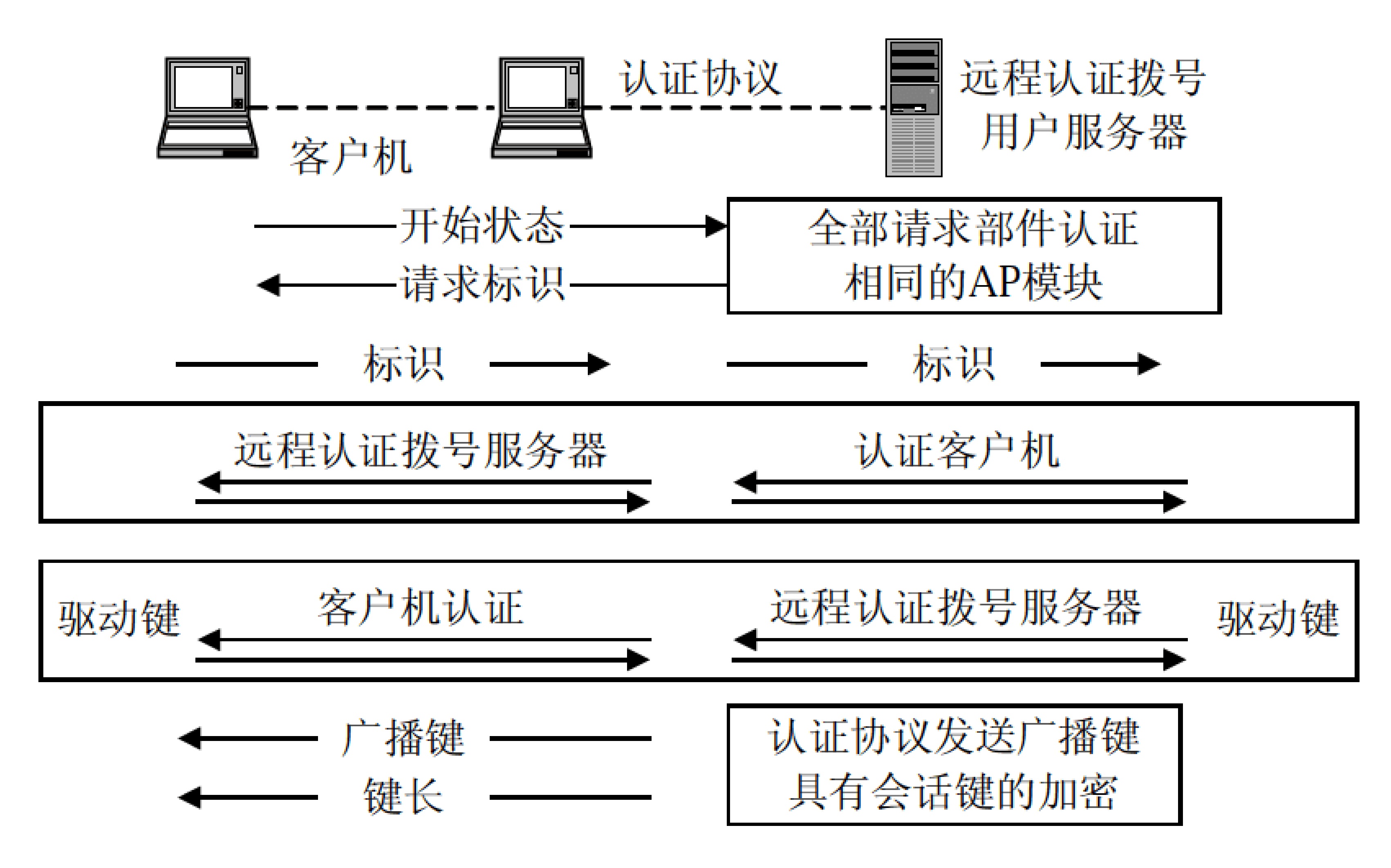


图 10-18　802.1X 组件间操作流程

由于 802.1X 是可扩展的，它允许在其上有多种认证算法。当前，为 802.11 所使用的 802.1X 没有规定某一种特定的算法，思科的解决方案中采用 LEAP。

10.6.4　LEAP 认证架构

思科设计的 LEAP 认证算法，提供了一种强壮的认证体系，并且非常易于实现。与其他的 EAP 认证算法一样，LEAP 被设计作为 802.1X 的上层。

（1）相互认证

由于无线终端缺乏有线的连接，在考虑网络认证用户的同时，用户也要对网络进行认证，思科的 LEAP 被设计实现双向认证。

（2）基于用户身份的认证

802.11 的认证是基于无线终端设备的，使用设备者的身份对网络认证点是不可见的，为避免设备丢失而造成的隐患，思科 LEAP 对使用设备者的身份进行认证。

（3）WEP 动态密钥管理

基于用户、双向认证的特点为用户管理、安全认证提供了很大方便，但依然需要一种机制来有效地管理 WEP 密钥——需要认证算法本身具备动态 WEP 密钥。LEAP 基于用户为每个无线终端生成唯一的密钥，大大减轻了网络管理者管理静态密钥的负担。802.1X 超时设定强制要求无线终端重新认证，从而继续维护网络的连接；而在算法中的重认证操作将支持动态 WEP 密钥的生成，这意味着用户的每一次重认证将开始使用新的 WEP 密钥。针对减轻统计密钥来源的攻击，这是一个非常关键的特点。

（4）临时密钥完整性协议 TKIP

前面的部分强调了 802.11 的安全隐患，尤其指出 WEP 是一种低功效的数据加密机制。思科采用即将标准化的方式（即众所周知的 TKIP）增强了 WEP 协议，从而减轻了现有的攻击并克服了其缺点。TKIP 是 802.11 工作组的标准草案，为最大程度上地保护现有用户对思科无线网络的投资，思科已经在产品方案上实施了 TKIP。

在对 WEP 增强方面，TKIP 主要包括两点：在所有 WEP 加密的数据包上采用报文完整性检测 MIC 功能，以更有效地保证数据帧的完整性；针对所有 WEP 加密的包实行基于每个数据包密钥的方式。此外，思科还增加了另外一种没有在 IEEE 802.11 工作组中定义的方式，称为 Broadcast Key Rotation。

（5）LEAP 认证流程

基于上面的 802.1X 的认证流程，LEAP 认证有以下增强。

当 Radius 认证服务器发送随意生成的认证报文到无线终端后，无线终端使用用户提供的密码进行单向加密，生成响应报文并发送回 Radius 认证服务器；认证服务器将使用数据库内的用户信息生成计算结果并与无线终端的响应结果相比较；认证服务器接受后，用户终端将认证网络的认证服务器，以上过程反向重复一次。

当最终双向认证成功，认证服务器将发送接收请求。当双向认证结束，Radius 认证服务器和无线终端将决定一个 WEP 密钥，它对无线终端是唯一的，并以此决定无线终端的网络接入级别，用户将用这个 WEP 密钥进行登录。在登录过程中，Radius 认证服务器通过有线网络发送这个动态点播 WEP 密钥（称为会话密钥）到接入点 AP，AP 将使用会话密钥去加密 AP 的广播密钥，并将加密后的广播 WEP 密钥发给无线终端。无线终端将使用会话密钥解出广播 WEP 密钥。

AP 和无线终端激活 WEP，并使用会话密钥和广播密钥为所有 AP 与无线终端间的数据包进行加/解密。会话密钥和广播密钥均可在一定的时间间隔内改变，该时间间隔可以被配置在 Radius 认证服务器上。这种认证方式为无线网络提供了最高级别的安全保证。

在实际的网络实施中，思科的 AP 可以使用多种不同的认证机制或类型，并在同一时间可以组合使用多种认证方式。不同的认证类型可以和 AP 配置的 SSID 结合，如果想在同

一个 AP 上同时为不同类型的终端提供服务，可以通过配置多个 SSID 来实现。

小　结

1. 无线网络标准

无线网络标准主要有：第二代蜂窝移动通信网、通信分组无线业务网、第三代蜂窝移动通信网、IEEE 802.11 无线局域网、HiperLan/2 高性能无线局域网、HomeRF 无线家庭网、蓝牙短距离无线网、IEEE 802.16 无线城域网。

2G（二代）移动通信系统采用数字信号实现语音和多种数据业务，主要有 GSM 和 CDMA 移动通信标准。GSM 采用 TDMA，具有 900MHz、1800MHz 和 1900MHz 3 个频段标准；CDMA 采用相互正交码型区分地址，能够在同一频率和同一时间下实现通信，从而比 GSM 有更大的容量。

通用分组无线业务网 GPRS 是 GSM 迈向 3G 的过渡移动通信标准，它采用分组交换传输模式。

ITU 将第三代移动通信命名为国际移动通信 IMT-2000，统一标准和频段，提高频谱利用率和支持多媒体通信是 3G 和 2G 的主要区别。

IEEE 802.11 WLAN 分为有固定基础设施和无固定基础设施两类；固定基础设施是指预先建立的基站或接入点（即 AP）；显然，无固定基础设施便是指没有安装 AP 的 WLAN。目前有 IEEE 802.11、802.11a、802.11b 和 802.11g 四个标准系列。

Hiper LAN/2 是宽带无线接入网 BRAN 的组成部分之一，物理层使用 5GHz ISM 频段和 OFDM 多载波调制技术，支持 6、9、12、18、27、30、54Mbps 多种传输速率。

Home RF 是 FCC 推出的面向家庭的无线网络工作标准，主要用于个人计算机和家用电子设备之间的无线通话。

蓝牙短距离无线网的蓝牙业界联盟特别兴趣小组 SIG 在全球范围内积极推广蓝牙技术，目前已推出 Bluetooth 1.0、Bluetooth 1.1、Bluetooth 2.03 个版本规范。

IEEE 802.16 标准系列是面向大范围覆盖的无线城域网标准，正式名称是固定宽带无线接入系统空中接口，微波接入全球互操作性 WiMAX 联盟正在致力于在全球范围内推广 IEEE 802.16 标准。

2. 无线局域网有线等价保密安全机制

有线等价保密 WEP 是 IEEE 802.11、IEEE 802.11a、IEEE 802.11b 和 IEEE 802.11g 无线局域网采用的安全保护机制。

WEP 加密与解密：初始密钥与 24 位初始向量 IV 连接后生成中间密钥，中间密钥通过 RC4 加密算法生成密钥流，密钥流与明文系统按位异或密文，这就是加密。WEP 解密是加密的逆过程。

IEEE 802.11 身份认证：表现在具有开放系统、封闭系统和共享密钥认证 3 种身份认证方式。

3．无线局域网有线等价保密安全漏洞

无线局域网有线等价保密安全漏洞有：WEP 默认配置漏洞、WEP 加密漏洞、WEP 密钥管理漏洞和服务设置标识漏洞。

4．无线局域网安全威胁

目前网络上有多种无线局域网探测和定位软件，也有许多软件工具支持无线局域网监听和密钥破译。无线局域网欺诈、无线 AP 欺诈和无线局域网劫持都是无线局域网的安全威胁。

5．无线保护接入安全机制

无线保护接入安全机制有 WPA 过渡标准和 IEEE 802.11i 标准。

WPA 的主要特点是采用 TKIP 加密技术代替了容易破译的 WEP 加密机制，将初始向量、密钥长度分别扩大到 48 位和 128 位；提供无线客户端双向认证功能，并使 WPA 向下兼容 WEP。IEEE 802.11i 的主要特点是支持 IEEE 802.1X、EAP 或 PSK，定义了 CCMP 和 WRAP 高级加密标准 AES。

6．无线网络安全实用技术举例

IEEE 802.11 规范的认证方式有两种：开放认证方式和共享密钥认证方式。但由于 MAC 地址被作为明文发送，所以入侵者很容易截获或假冒有效的无线终端。

思科无线网络安全套件由 802.1X 认证体系、LEAP 认证算法、临时密钥完整性协议 TKIP、报文完整性检测 MIC 等几部分组成。

802.1X 认证架构已经被采用在 IEEE 802.11 工作组 I（TGI）中作为 802.11 MAC 层安全的增强手段。

思科设计的 LEAP 认证算法提供了一种强壮的认证体系，并且非常容易实现。

练习与思考

1．简述 IEEE 802.11 WLAN 开放系统认证和共享密钥认证的过程及各自的特点。
2．WEP 主要有哪些安全漏洞？
3．为什么获得足够多的相同初始向量，就有可能从密文消息中破译出密钥？
4．无线局域网主要有哪些安全威胁？
5．“战争驱车探测”软件 NetStumbler 可以获得目标 WLAN 的哪些信息？
6．分别简述共享密钥认证欺诈过程和封闭系统认证 MAC 地址欺诈过程。
7．WPA 采用哪些技术加强了 WLAN 的安全性？
8．IEEE 802.11i 标准提出的健壮安全网络概念主要包含哪些内容？

9．列举 WEP 安全机制的优缺点。

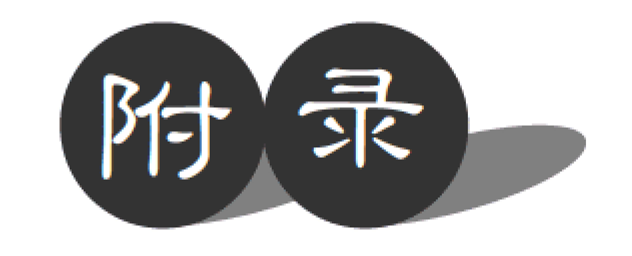
10．列举 WPA 安全机制的优缺点。

11．试述 IEEE 802.11i 安全机制的优缺点。

12．试述 WEP、WPA 和 IEEE 802.11i 标准的异同。

13．思科设计的 LEAP 认证算法包含哪些内容？

14．思科无线网络安全套件由哪几部分组成？



对网络安全实验的建议及题目

1. 对网络安全实验的一些建议

（1）进行市场调查。找一家计算机配件商店，了解一下各种网卡的价格。例如，10Mbps、100Mbps、1000Mbps 和 10/100Mbps 等各种导线的价格。又例如，粗同轴电缆、3 类双绞线、5 类屏蔽和无屏蔽双绞线，网络插头（水晶头）和电话线插头等的价格。

（2）使用剪线钳和剥线钳制作一些 5 类无屏蔽双绞线的 RJ-45 连接器，并使用电缆测试仪检查是否合格，以备做实验使用。

（3）如果学校没有网络安全实验室，应该配置一些路由器和相应层次的交换机、无线接入设备、光纤等传输媒体供实验之用。由学生自己组建网络安全实验室。

（4）在实验室的互联网上用不同的计算机复制文件，设置不同的共享情况进行复制。

（5）在客户机上制作一个网页，并发送到实验室服务器上；从另一台客户机的某个文档链接到上述网页。

（6）建议所有的网络安全实验均由两名学生相互合作完成。

2. 网络安全实验题目

囿于篇幅限制，在此不可能详细介绍实验内容、实验目的和实验步骤，只能列举一些实验的题目。每个题目的实验目的、原理简介、实验环境、实验步骤、实验报告和思考题等内容参见相关的计算机网络安全实验教程。本书要求最少做 12 个实验。

（1）路由器配置

（2）VLAN 划分

（3）DES 算法

（4）加密软件 PGP 的应用

（5）DSS 数字签名算法

（6）嗅探器的实现

（7）端口扫描

（8）木马的安装及使用

（9）安全策略设置

（10）系统安全扫描
（11）IPSec 安全配置
（12）Linux 操作系统用户管理
（13）Linux 操作系统文件权限管理
（14）Web 服务器的设置
（15）Web 服务器的安全设置
（16）Linux 环境下 IPSec VPN 的实现
（17）在 Windows 下搭建入侵检测平台
（18）在 Windows 2003 Server 环境下独立根 CA 的安装及使用
（19）无线局域网安全实验
（20）防火墙的非法数据流处理能力测试

英文缩写对照表

A

AAA	authentication, authorization, accounting	认证、授权、审计
AAFID	autonomous agents for intrusion detection	入侵检测自治代理
ACL	access control table	访问控制列表
AES	advanced encryption standard	高级加密标准
AH	IP authentication header	IP 认证包头
AirCERT	automated incident reporting	自动事件报告
AP	access point	接入点
ARP	address resolution protocol	地址解析协议
ASA	adaptive security algorithm	自适应安全算法

B

BEEP	blocks extensible exchange protocol	块扩展交换协议
BIND	Berkeley Internet name domain	伯克利 Internet 名字域
BPF	Berkeley packet filter	伯克利数据包过滤器
BRAN	broadband radio access networks	宽带无线接入网
BSM	basic security module	基础安全模块
BSS	basic service set	基本服务集

C

CA	computer associates international	国际计算机联盟
CAN	cipher and authentication negotiation	密码和认证协商
CBC- MAC	cipher block chaining message authentication code	密码块链接消息认证码
CC	common criteria for information technology security evaluation	信息技术安全评价公共标准

CCMP	counter-mode/CBC- MAC protocol	计数模式/CBC-MAC 协议
CCRA	common criteria recognition arrangement	多边认可协议
CDMA	code division multiple access	码分多址
CERT	CERT Coordination Center	计算机应急响应协作中心
CIDF	common intrusion detection framework	通用入侵检测框架
CISL	common intrusion specification language	通用入侵规范语言
CMU	Carnegie Mellon University	卡耐基・梅隆大学
CSMA/CD	carrier sense multiple access/collision detect	载波监听多路访问/冲突检测
CSPF	CMU Stanford packet filter	卡耐基・斯坦福数据包过滤器
CTCPEC	Canadian trusted computer product evaluation criteria	加拿大可信计算机产品评价标准
CVE	common vulnerability and exposures	公共漏洞披露机构
CyberCop	CyberCop intrusion protection	入侵防护系统

D

DAC	discretionary access control	自主访问控制
DACL	discretionary access control list	自主访问控制列表
DARPA	Defense Advanced Research Projects Agency	美国国防部高级研究计划署
DDoS	distributed denial of service	分布式拒绝服务攻击
DECT	digital enhanced cordless telephony	数字增强无绳电话
DES	data encryption standard	数据加密标准
DET	detection error tradeoff	检测误差权衡曲线
DIDS	distributed intrusion detection system	分布式入侵检测系统
DMZ	demilitarized zone	非军事区
DNS	domain name systems	域名系统
DoS	denial of service	拒绝服务
DSSS	direct sequence spread spectrum	直序扩频

E

EAL	evaluation assurance levels	评价保证等级
EAP	enhanced authentication protocol	扩展认证协议
EDR	enhanced data rate	增强数据率
EL	event logger	事件记录器
ESP	IP encapsulating security payload	IP 封装安全负载
ESS	extended service set	扩展服务集
ETSI	European Telecommunication Standard Institute	欧洲电信标准协会

F

FC	Federal Criteria for Information Technology Security	信息技术安全评价联邦标准
FCC	Federal Communications Commission	联邦通信委员会
FDD	frequency division duplex	频分双工
FDMA	frequency division multiple address	频分多址

FHSS	frequency hopping spread spectrum	跳频扩频
FPLMTS	future public land mobile telecommunication systems	未来公众陆地移动电信系统
FTP	file transfer protocol	文件传输协议

G

GIDO	general intrusion detection object	通用入侵检测对象
GISA	German Information Security Agency	德国信息安全部
GPS	global position system	全球定位系统
GRE	generic routing encapsulation	通用路由协议封装
GSM	global system for mobile communication	全球移动通信系统

H

H2GF	HiperLAN/2 Global Forum	HiperLAN/2 全球论坛
HIDS	host-based intrusion detection system	主机入侵检测系统
HiperLAN	high performance radio local area network	高性能无线局域网
HMM	hidden Markov model	隐马尔科夫模型
HomeRF	home radio frequency	家庭无线网络
HR-DSSS	high rate direct sequence spread spectrum	高速率直序扩频
HTML	hypertext markup language	超文本标志语言
HTTP	hypertext transfer protocol	超文本传输协议

I

IBSS	independent basic service set	独立基本服务集
ICMP	Internet control messages protocol	Internet 控制报文协议
ICV	integrity check value	完整性校验值
IDEA	international data encryption algorithm	国际数据加密算法
IDES	intrusion detection expert system	入侵检测专家系统
IDWG	intrusion detection working group	入侵检测工作组
IDMEF	intrusion detection message exchange format	入侵检测消息交换格式
IDS	intrusion detection system	入侵检测系统
IDSM	intrusion detection system module	入侵检测系统模块
IDXP	intrusion detection exchange protocol	入侵检测交换协议
IEC	International Electrotechnical Commission	国际电工委员会
IETF	Internet Engineering Task Force	因特网工程任务组
IGMP	Internet group management protocol	Internet 组管理协议
IKE	Internet key exchange	Internet 密钥交换
IMAP4	Internet message access protocol version4	消息访问协议版本 4
IMT-2000	International Mobile Telecmmunication-2000	国际移动电信
InterNIC	Internet Network Information Center	Internet 网络信息中心
IP	Internet protocol	网际协议

IPSec	IP security protocol	IP 安全协议
IR	infrared	红外线
ISAKMP	Internet security association and key management protocol	Internet 安全关联和密钥管理协议
ISM	industry science and medical	工业、科学和医疗频段
ISN	initial sequence number	初始序列号
ISO	International Organization for Standardization	国际标准化组织
ISS	Internet Security Systems	因特网安全系统公司
ITSEC	information technology security evaluation criteria	信息技术安全评价标准
ITU	International Telecommunication Union	国际电信联盟
IV	initialization vector	初始向量
	K	
KH	key hierarchy	密钥体系
KM	key management	密钥管理
	L	
L2F	layer 2 forwarding	第二层转发协议
L2TP	layer2 tunneling protocol	第二层隧道协议
Libpcap	packet capture library	数据包捕获函数库
LSA	local security authority	本地安全认证
	M	
MAC	mandatory access control	强制访问控制
MAC	medium access control	介质访问控制
MIC	message integrity check	消息完整性校验
MIME	multipurpose Internet mail extensions	多用途邮件扩展协议
MPLS	multi protocol label switching	多协议标记交换
MPPE	microsoft point to point encryption	微软点对点加密算法
MSS	maximum segment size	最大数据段大小
MTA	message transfer agent	报文传送代理
MTU	maximum transmission unit	最大传输单元
	N	
NAI	Network Associates Inc.	网络联盟有限公司
NAS	network access server	网络接入服务
NAT	network address translator	网络地址转换
NCSC	National Computer Security Center	美国国家计算机安全中心
NetBIOS	network basic input output system	网络基本输入输出系统
NIDES	next-generation intrusion detection expert system	下一代入侵检测专家系统
NIDS	network-based intrusion detection system	网络入侵检测系统
NIST	National Institute of Standards and Technology	美国国家标准技术委员会
NSA	National Security Agency	美国国家安全局

NSM	network security monitor	网络安全监视器

O

OFDM	orthogonal frequency division multiplexing	正交频分复用
OPSEC	open platform for security	安全性开放式平台
OSSIM	open source security information management	开放源码安全信息管理系统
OUI	organizationally unique identifier	厂商唯一标识

P

PA	pre-authentication	预先认证
PEM	privacy enhancement for Internet electronic mail	保密增强 Internet 邮件
PIX	private internet exchange	保密互联交换
POP3	post office protocol-version3	邮局协议-版本 3
PP	protection profile	保护轮廓
PPP	point to point protocol	点对点协议
PPTP	point to point tunnel protocol	点对点隧道协议
PRNG	pseudo random number generator	随机数生成器
PSK	pre-shared key	预先共享密钥

Q

QoS	quality of service	服务质量

R

RADIUS	remote authentication dial-in user service	远程认证拨号用户服务
RAID	redundant arrays of inexpensive disks	冗余磁盘阵列
RARP	reverse address resolution protocol	逆向地址解析协议
RDP	reliable data protocol	可靠数据报协议
RIPPER	repeated incremental pruning to produce error reduction	重复增量裁剪缩减错误
RISC	reduced instruction system computer	精简指令系统计算机
ROC	receiver operating characteristic	接收机操作特性曲线
RPC	remote procedure call	远程过程调用
RSA	Ron Rivest, Adi Shamir, Leonard Adleman	以人名命名的加密算法
RSN	robust security network	健壮安全网络

S

SA	security association	安全关联
SACK	selective acknowledgement	选择性应答
SACL	system access control list	系统控制访问列表
SAD	security association database	安全关联数据库
SAM	security account management	安全账户管理
SET	secure electronic transaction	安全电子交易协议
SF	security target	安全目标

SID	subject identification	主体安全标识符
SIG	Bluetooth Special Interest Group	蓝牙特别兴趣小组
SII	standard indicator icons	标准批示图标
SMB	server message block	服务器消息块协议
SMTP	simple message transfer protocol	简单邮件传输协议
SOHO	small office home office	小型或家庭办公
SPAN	switched port analyzer	交换端口分析器
SPD	security policy database	安全策略数据库
SPI	security parameters index	安全参数索引
SPI	stateful packet inspection	状态包检查
SRI	Stanford Research Institute	斯坦福研究所
SRM	security reference monitor	安全参考监视器
SSID	service set identity	服务设置标识
SSL	security socket layer	安全套接层
SVM	support vector machine	支持向量机
SWAP	shared wireless access protocol	共享无线访问协议

T

TAP	test access port	测试接入端口
TCP	transfer control protocol	传输控制协议
TCSEC	trusted computer system evaluation criteria	可信计算机系统评价标准
TDD	time division duplex	时分双工
TDI	trusted database interpretation	可信数据库解释
TDMA	time division multiple address	时分多址
TD-SCDMA	time division-synchronous CDMA	时分同步 CDMA
TEMPEST	transient electromagnetic pulse emanation standard	瞬态电磁脉冲辐射标准
TKIP	temporal key integrity protocol	临时密钥完整性协议
TLS	transport layer security	传输层安全
TNI	trusted network interpretation	可信网络解释
TOE	target of evaluation	评价目标
TTL	time to live	生存时间

U

UA	user agent	用户代理
UDP	user datagram protocol	用户数据报协议

V

VPN	virtual private networking	虚拟专用网

W

WCDMA	wideband CDMA	宽带 CDMA

WECA	wireless Ethernet Compatibility Alliance	无线以太网兼容性联盟
WEP	wired equivalent privacy	有线等价保密
Wi-Fi	Wireless Fidelity Alliance	无线高保真联盟
WiMAX	Worldwide Interoperability for Microwave Access	微波接入全球互操作性联盟
WLAN	wireless local area network	无线局域网
WLL	wireless local loop	无线本地回路
WMAN	wireless metropolitan area network	无线城域网
WPA	Wi-Fi protected access	无线保护接入
WPA2	Wi-Fi protected access2	第二代无线保护接入
WPAN	wireless personal area network	无线个人区域网
WRAP	wireless robust authenticated protocol	无线健壮认证协议

X

XML	extensible markup language	可扩展标记语言

中国安全信息网：http://www.hacker.cn。

中国协议分析网：http://www.cnpaf.net。

网络安全焦点：http://www.xfocus.net。

20cn 网络安全小组：http://www.20cn.net。

国家计算机网络应急技术处理协调中心：http://www.cert.org.cn。

国家信息安全测评中心：http://www.itsec.gov.cn。

ISA 中文网站：http://www.isacn.org。

中国信息安全认证中心：http://www.isccc.gov.cn。

国际计算机安全联合会：http://www.trusecure.com。

中国鹰派联盟：http://www.chinawill.com。

国际 PGP 网站：http://www.pgpi.org。

赛迪网技术应用：http://tech.ccident.com/pub/column/c1100.html。

参考文献

[1] 胡道元，闵京华．网络安全．北京：清华大学出版社，2004
[2] 彭新光，吴兴兴．计算机网络安全技术与应用．北京：科学出版社，2006
[3] 刘远生．计算机网络安全．北京：清华大学出版社，2006
[4] 刘建伟，张卫东等．网络安全实验教程．北京：清华大学出版社，2007
[5] 冯元，兰少华．计算机网络安全基础．北京：科学出版社，2003
[6] 韩乐海，王超．入侵检测系统实例剖析．北京：清华大学出版社，2002
[7] 胡建伟．网络安全与保密．西安：西安电子科技大学出版社，2003
[8] 姜楠，王健．移动网络安全技术与应用．北京：电子工业出版社，2004
[9] 彭新光，王峥．入侵检测分类引擎预测精度度量方法．计算机工程，2004，30（4）
[10] 卿斯汉，刘文清．操作系统安全导论．北京：科学出版社，2003
[11] 许榕生，刘宝旭．黑客攻击技术揭密．北京：机械工业出版社，2002
[12] 袁津生，吴砚农．计算机网络安全基础．北京：人民邮电出版社，2004
[13] 张友生，米安然．计算机病毒与木马程序．北京：北京科海电子出版社，2003
[14] 叶忠杰，陈月波等．计算机网络安全技术．北京：北京科学技术出版社，2003
[15] 顾巧论，蔡振山等．计算机网络安全．北京：北京科学技术出版社，2006
[16] 徐茂智，游林．信息安全与密码学．北京：清华大学出版社，2007
[17] 单新建．计算机病毒原理及防治．北京：北京邮电大学出版社，2004
[18] 李涛．网络安全概论．北京：电子工业出版社，2004
[19] 梁亚声．计算机网络安全技术教程．北京：机械工业出版社，2004
[20] 陈明．网络安全教程．北京：清华大学出版社，2004
[21] 张千里等．网络安全新技术．北京：人民邮电出版社，2003
[22] 王竹林等．网络安全实践．西安：电子科技大学出版社，2002
[23] 郭世强等．网络安全技术与应用大典．北京：人民邮电出版社，2003
[24] 林海等．计算机网络安全．北京：高等教育出版社，2002
[25] 雷渭侣，王兰波等．计算机网络．北京：机械工业出版社，2008
[26] 雷渭侣，张毓森等．数据通信与计算机网络．北京：解放军出版社，2002
[27] 雷渭侣，王兰波等．计算机网络应用技术．广州：华南理工大学出版社，2006
[28] 谢希仁．计算机网络教程．第 2 版．北京：人民邮电出版社，2006
[29] 阚喜成，孙锐等．信息安全原理及应用．北京：清华大学出版社，2006
[30] 丁宇，林其．网络管理与维护．北京：冶金工业出版社，2006

[31] Andrew S．Tanenbaum．Computer Networks．3rd ed（影印版）．北京：清华大学出版社，1996

[32] Douglas Comer．Computer Networks and Internet（影印版）．北京：清华大学出版社，1998

[33] William Stallings．Data and Computer Communications．5th ed（影印版）．北京：清华大学出版社，1998

[34] Christian Barnes．无线网络安全防护（影印版）．北京：机械工业出版社，2003

[35] Greg Holden．防火墙与网络安全（影印版）．北京：清华大学出版社，2004

[36] Keith EStrassherg．防火墙技术大全（影印版）．北京：机械工业出版社，2003